

Jabber SIP URI-Anrufe über MRA

Inhalt

[Einführung](#)

[Szenario](#)

[Annahmen](#)

[Konfiguration in Organisation 1, wenn Jabber A Jabber B anruft](#)

[Der gesamte Ablauf ausgehender Anrufe wird](#)

[Konfiguration in Organisation 1, wenn Jabber B Jabber A anruft](#)

[Der gesamte eingehende Anruffluss wird](#)

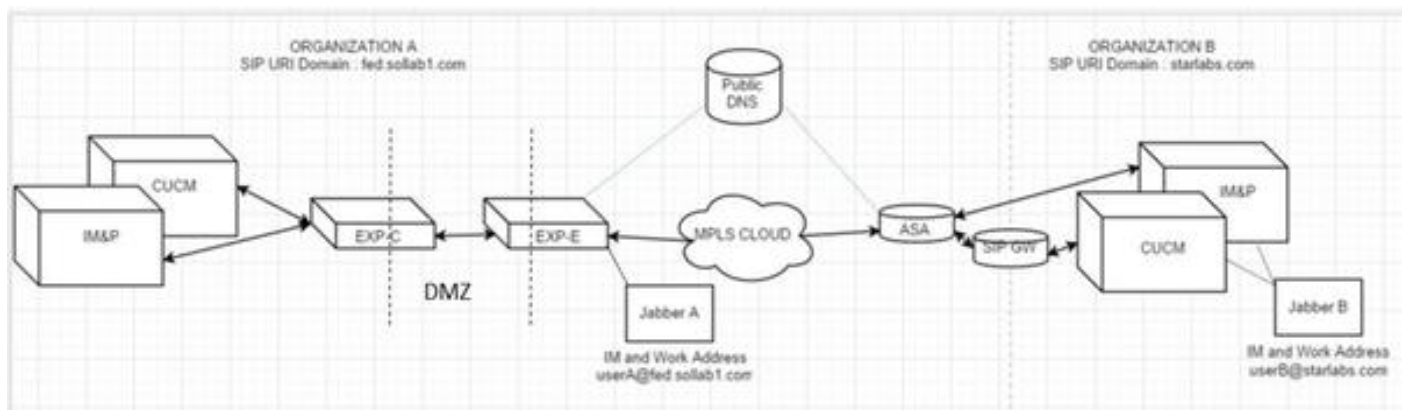
Einführung

In diesem Dokument wird die Konfiguration von Cisco Unified Communications Manager (CUCM) sowie Expressway C und E beschrieben, sodass Jabber den Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) eines anderen Benutzers aus einer anderen Organisation aufrufen kann, wenn er über MRA (Mobile Remote Access) verbunden wird. Dasselbe im Kontext von Expressway wird auch B2B-Anrufablauf genannt.

Szenario

Angenommen, Organisation 1 verwendet MRA, Organisation 2 dagegen nicht. Für Organisation 2 endet der Perimeter mit einer Adaptive Security Appliance (ASA), hinter der CUBE steht, das in CUCM-Cluster von Organisation 2 integriert ist.

Wie im Bild gezeigt, kann Jabber A über MRA oder intern verbunden werden. Die Konfiguration für CUCM, Expressway C und E für Organisation 1 bleibt jedoch gleich.



Annahmen

Sie können davon ausgehen, dass Jabber A-Benutzer und Jabber B-Benutzer IM und Presence

über eine XMPP-Föderation (Extensible Messaging and Presence Protocol) austauschen können, und dass ihre IM-Adressen auch ihre Arbeits-SIP-URIs sind.

Jabber A und Jabber B können darüber hinaus intern über SIP URI in ihren jeweiligen Organisationen erfolgreich gewählt werden.

Im obigen Szenario gehen Sie davon aus, dass Organisation 2 CUCM als Anrufsteuerungsserver verwendet. Dabei kann es sich jedoch auch um einen Anrufsteuerungsserver eines anderen Anbieters handeln.

Bei der Integration von CUCM, Jabber und VCS für MRA muss die Version bekannt sein.

Konfiguration in Organisation 1, wenn Jabber A Jabber B anruft

Schritt 1: Erstellen Sie ein neues SIP-Trunk-Sicherheitsprofil mit dem Überwachungsport 5065, wie im Bild gezeigt:

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status: Ready

SIP Trunk Security Profile Information

Name*	VCS SIP Trunk Profile
Description	VCS SIP Trunk Profile non-secure
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5065
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Schritt 2: Erstellen Sie einen SIP-Trunk, der auf ExpressWay-C verweist, und weisen Sie das SIP-

Trunk-Sicherheitsprofil zu, wie im Bild gezeigt:

SIP Information

- Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.82.114		5060

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* VCS SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile For Cisco VCS [View Details](#)

DTMF Signaling Method* RFC 2833

- Normalization Script

Hinweis: Es wird ein neues Trunk-Sicherheitsprofil erstellt, das den 5065-Port abhört. Er wird diesem neuen SIP-Trunk zugewiesen, der auf Expressway-C verweist, da Expressway-C bereits so konfiguriert ist, dass er Jabber Un-Secure Registrierungen für 5060 an CUCM sendet, wenn sich der Jabber-Benutzer über MRA anmeldet. Wenn Sie das Standard-Trunk-Sicherheitsprofil verwenden, kann sich Jabber, der über MRA angemeldet ist, nicht auf Port 5060 des CUCM registrieren.

Schritt 3: Erstellen Sie das SIP-Routenmuster für den URI von Organisation 2, und weisen Sie diesen dem SIP-Trunk-Punkt Expressway-C zu, wie im Bild gezeigt:

SIP Route Pattern Configuration

Save Delete Copy Add New

Status

Status: Ready

Pattern Definition

Pattern Usage Domain Routing

IPv4 Pattern* starlabs.com

IPv6 Pattern

Description VCS MRA calls

Route Partition < None >

SIP Trunk/Route List* VCS-MRA-TRNK

Block Pattern

Schritt 4: Erstellen Sie eine Nachbarzone auf Expressway-C, die auf CUCM verweist, wie im Bild gezeigt:

The image shows a configuration interface for a Cisco Expressway. It is divided into three sections: Configuration, H.323, and SIP. Each section has a title bar and a list of settings.











- Configuration**
 - Name: CUCM-ORG1
 - Type: Neighbor
 - Hop count: 15
- H.323**
 - Mode: Off
- SIP**
 - Mode: On
 - Port: 5065
 - Transport: TCP
 - Accept proxied registrations: Deny
 - Media encryption mode: Auto
 - ICE support: Off

Schritt 5: Erstellen Sie auf dem Expressway-C eine Traversal-Client-Zone (keine UC-Traversal), wie im Bild gezeigt:

Type	Traversal client
Hop count	★ 15 ⓘ
Connection credentials	
Username	★ cisco ⓘ
Password	★ ●●●●●●●● ⓘ
H.323	
Mode	Off ⓘ
SIP	
Mode	On ⓘ
Port	★ 7003 ⓘ
Transport	TCP ⓘ
Accept proxied registrations	Allow ⓘ
Media encryption mode	Auto ⓘ
ICE support	Off ⓘ
SIP noison mode	Off ⓘ

Schritt 6: Erstellen Sie auf dem Expressway-E eine Traversal-Serverzone (keine UC-Traversal), wie im Bild gezeigt:

Edit zone

Type	Traversal server
Hop count	15 
Connection credentials	
Username	cisco 
Password	Add/Edit local authentication database
H.323	
Mode	Off 
SIP	
Mode	On 
Port	7003 
Transport	TCP 
Accept proxied registrations	Allow 
Media encryption mode	Auto 
ICE support	Off 
...	Off 

Schritt 7: Erstellen Sie eine DNS-Zone auf Expressway-C, die für eine DNS SRV-Suche nach dem URI von Organisation 2 verwendet wird, wie im Bild gezeigt:

Configuration	
Name	★ VCS-MRA-DNS ⓘ
Type	DNS
Hop count	★ 15 ⓘ

H.323	
Mode	Off ▼ ⓘ

SIP	
Mode	On ▼ ⓘ
TLS verify mode	Off ▼ ⓘ
Fallback transport protocol	UDP ▼ ⓘ
Media encryption mode	Auto ▼ ⓘ
ICE support	Off ▼ ⓘ

Sobald alle Zonen eingerichtet sind, müssen Sie Suchregeln auf Expressway C und E definieren, damit das Routing stattfinden kann.

Schritt 8: Die Suchregel für Expressway-C besteht darin, die **SIP-Einladung** für URI starlabs.com an Expressway-E weiterzuleiten, in der neuen Traversal Zone, die Sie erstellt haben, wie im Bild gezeigt:

Configuration	
Rule name	★ Inside-to-Outside-MRA-CUCMORG2 ⓘ
Description	ⓘ
Priority	★ 99 ⓘ
Protocol	SIP ▼ ⓘ
Source	Any ▼ ⓘ
Request must be authenticated	No ▼ ⓘ
Mode	Alias pattern match ▼ ⓘ
Pattern type	Regex ▼ ⓘ
Pattern string	★ .*@starlabs.com\$ ⓘ
Pattern behavior	Leave ▼ ⓘ
On successful match	Continue ▼ ⓘ
Target	★ b2b ▼ ⓘ
State	Enabled ▼ ⓘ

Schritt 9: Suchregel auf Expressway-E , um die **SIP-Einladung** für URI starlabs.com an die DNS-ZONE weiterzuleiten, sobald der Anruf Expressway-Evia über die Traversal-Zone erreicht hat, die Sie vorgenommen haben, wie im Bild gezeigt:

Rule name	CUCM to VCSe to DNS
Description	VCS MRA calls
Priority	130
Protocol	SIP
Source	Named
Source name	b2b
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	*@starlabs.com\$
Pattern behavior	Leave
On successful match	Continue
Target	VCS-MRA-DNS
State	Enabled

Schritt 10: Sobald der Anruf die DNS-Zone erreicht hat, führt Expressway-C eine DNS SRV-Suche für **_sips.tcp.starlabs.com**, **_sip._tcp.starlabs.com** und **_sip.udp.starlabs.com** gegenüber dem öffentlichen DNS-Server durch.

In den Exp-E-Protokollen wird Folgendes angezeigt:

```
2016-03-09T09:48:35+05:30 VCSECOL tvcs: UTCTime="2016-03-09 04:18:35,399" Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="_sip._tcp.starlabs.com" Type="SRV (IPv4 and IPv6) "
```

```
2016-03-09T09:48:35+05:30 VCSECOL tvcs: UTCTime="2016-03-09 04:18:35,400" Module="network.dns" Level="DEBUG": Detail="Resolved hostname to: ['IPv4''TCP''14.160.103.10:5060'] (A/AAAA) Number of relevant records retrieved: 1"
```

Von der DNS-SRV-Suche erhält Exp-E die IP-Adresse und den Port für den nächsten Hop, um die Organisation 2 zu erreichen. In diesem Szenario wird DNS SRV **_sip._tcp.starlabs.com** in den öffentlichen FQDN/IP und Port 5060 der ASA für Organisation 2 aufgelöst.

Der gesamte Ablauf ausgehender Anrufe wird

1. Jabber A wählt **userB@starlabs.com** als SIP URI.
2. SIP Invite erreicht CUCM (über Exp-E → Exp-C).
3. Der CUCM führt eine Zifferanalyse durch, die mit dem **SIP-Routenmuster** übereinstimmt.
4. CUCM leitet den Anruf über einen SIP-Trunk an Exp-C weiter.

5. Exp-C erhält den Anruf in der "CUCM Neighbor Zone" und die "Search Rule" leitet den Anruf an die Traversal-Zone weiter, die wir eingerichtet haben.
6. Der Anruf erreicht jetzt die Exp-E über die Traversal-Zone, und die Suchregel leitet den Anruf an die DNS-Zone weiter.
7. Wenn die DNS-Zone erreicht ist, wird die DNS SRV-Suche nach `_sip._tcp.starlabs.com` für den öffentlichen DNS-Server ausgeführt, der zum nächsten Hop für die Erreichbarkeit von Organisation 2 aufgelöst wird.

Konfiguration in Organisation 1, wenn Jabber B Jabber A anruft

Nehmen wir an, Organisation 2 hat einen eigenen Wählplan, der so konfiguriert ist, dass ein SIP URI-Anruf an Organisation 1 weitergeleitet wird, wenn Jabber B Jabber A anruft. Sehen wir uns an, welche Änderungen Sie benötigen, um die eingehende SIP-INVITE-Nachricht an den CUCM von Organisation 1 weiterzuleiten.

Schritt 1: Eingehende Suchregel für Expressway-E zum Senden einer eingehenden SIP-Einladung von Organisation 2 an Exp-C für die SIP-URI-Domäne **feed.sollab1.com**, wie im Bild gezeigt:

The screenshot shows the configuration for a Search Rule in CUCM. The rule is named "VCS to VCSc to CUCM" and has the description "VCS MRA calls from outside". The priority is set to 120. The protocol is SIP, and the source is set to "Any". The request must not be authenticated. The mode is "Alias pattern match" and the pattern type is "Regex". The pattern string is `.*@fed.sollab1.com$`. The pattern behavior is set to "Leave" and the action on a successful match is "Continue". The target is set to "b2b" and the rule is enabled.

Configuration	Value
Rule name	VCS to VCSc to CUCM
Description	VCS MRA calls from outside
Priority	120
Protocol	SIP
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	.*@fed.sollab1.com\$
Pattern behavior	Leave
On successful match	Continue
Target	b2b
State	Enabled

Schritt 2: Eingehende Suchregel auf Expressway-C, zum Senden einer eingehenden SIP-Einladung von Exp-E an CUCM, für die SIP URI-Domäne **feed.sollab1.com**, wie im Bild gezeigt:

Configuration	
Rule name	★ Outside-to-Inside-MRA
Description	VCS MRA calls from outside
Priority	★ 98 ⓘ
Protocol	SIP ⓘ
Source	Named ⓘ
Source name	★ b2b ⓘ
Request must be authenticated	No ⓘ
Mode	Alias pattern match ⓘ
Pattern type	Regex ⓘ
Pattern string	★ .*@fed.sollab1.com\$ ⓘ
Pattern behavior	Leave ⓘ
On successful match	Continue ⓘ
Target	★ CUCM-ORG1 ⓘ
State	Enabled ⓘ

Der gesamte eingehende Anruffluss wird

1. Eingehende SIP-EINLADUNG von Jabber B für **userA@fed.sollab1.com** trifft Exp-E.
2. Die Suchregel auf Exp-E leitet den Anruf über die Traversal-Zone an Exp-C weiter.
3. Suchregel auf Exp-C , leitet den Anruf über die "CUCM Neighbor Zone" an den CUCM-Cluster weiter.
4. CUCM sendet die SIP-Einladung an Jabber A, registriert über MRA (via Exp-C → Exp-E).

Hinweis: Für B2B-Anrufe werden Rich Media-Lizenzen sowohl auf ExpressWay-C als auch auf ExpressWay-E benötigt.

Hinweis: Stellen Sie sicher, dass der Kunde die richtigen Ports an der Firewall geöffnet hat.