

MRA를 통한 Jabber SIP URI 통화

목차

[소개](#)

[시나리오](#)

[가정](#)

[Jabber A가 Jabber B를 호출할 때 조직 1의 구성](#)

[전체 아웃바운드 통화 흐름은](#)

[Jabber B가 Jabber A를 호출할 때 조직 1의 구성](#)

[전체 인바운드 통화 흐름은](#)

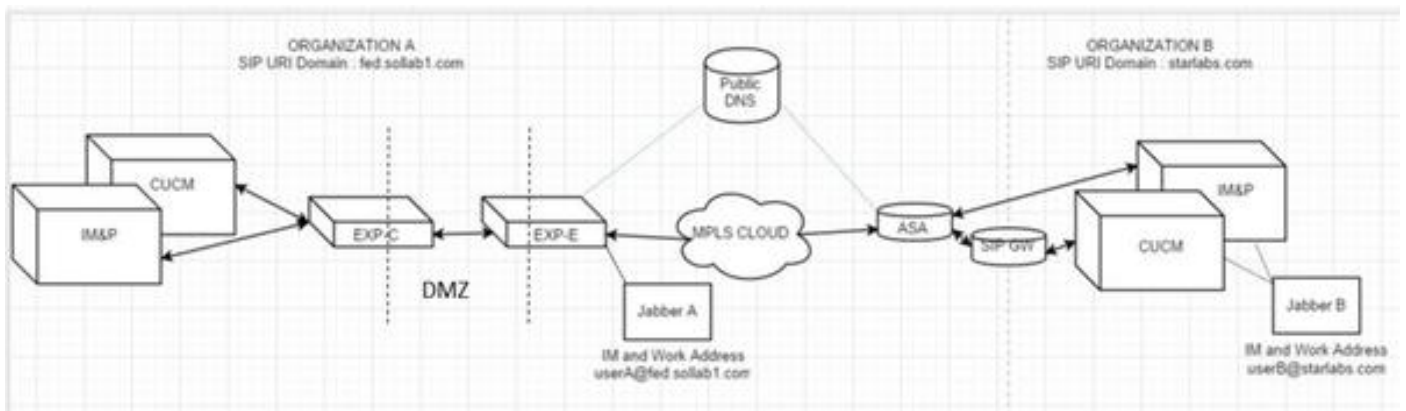
소개

이 문서에서는 Jabber가 MRA(Mobile Remote Access)를 통해 연결할 때 다른 조직의 다른 사용자의 SIP(Session Initiation Protocol) URI(Uniform Resource Identifier)를 호출할 수 있도록 Cisco CUCM(Unified Communications Manager) 및 Expressway C 및 E와 관련된 컨피그레이션에 대해 설명합니다. Expressway의 컨텍스트에서는 B2B 통화 흐름이라고도 합니다.

시나리오

조직 1이 MRA를 배포하고 조직 2가 구축하지 않는 시나리오를 가정해보겠습니다. 조직 2의 경우, 경계는 ASA(Adaptive Security Appliance)로 끝납니다. 이 외에도 조직 2의 CUCM 클러스터와 통합된 CUBE가 있습니다.

이미지에 표시된 것처럼 Jabber A는 MRA를 통해 또는 내부적으로 연결할 수 있지만, 조직 1의 경우 CUCM, Expressway C 및 E에서 컨피그레이션은 동일하게 유지됩니다.



가정

Jabber A 사용자 및 Jabber B 사용자는 XMPP(Extensible Messaging and Presence Protocol) 페더레이션을 통해 IM 및 프레전스를 교환할 수 있으며, 해당 IM 주소도 작업 SIP URI라고 가정할 수 있

습니다.

또한 Jabber A와 Jabber B는 해당 조직 내에서 내부적으로 SIP URI를 통해 다이얼할 수 있습니다.

위의 시나리오에서 조직 2에 통화 제어 서버로 CUCM이 있다고 가정합니다. 그러나 다른 공급업체의 통화 제어 서버일 수도 있습니다.

CUCM, Jabber, VCS for MRA를 통합하는 동안 버전에 대한 인식이 필요합니다.

Jabber A가 Jabber B를 호출할 때 조직 1의 구성

1단계. 이미지에 표시된 대로 수신 대기 포트 5065가 있는 새 SIP 트렁크 보안 프로필을 생성합니다

The screenshot shows the 'SIP Trunk Security Profile Configuration' window. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the status is 'Ready'. The main section is titled 'SIP Trunk Security Profile Information' and contains the following fields and options:

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

2단계. 이미지에 표시된 대로 ExpressWay-C를 가리키는 SIP 트렁크를 생성하고 SIP 트렁크 보안 프로필을 할당합니다.

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


참고: 5065 포트에서 수신하는 새 트렁크 보안 프로파일이 생성됩니다. Expressway-C는 Jabber 사용자가 MRA를 통해 로그인할 때 5060에서 CUCM에 Jabber Unsecure 등록을 전송하도록 이미 구성되어 있으므로 Expressway-C를 가리키는 이 새 SIP 트렁크에 할당됩니다. 기본 트렁크 보안 프로필을 사용하는 경우 MRA를 통해 로그인한 Jabber가 CUCM의 포트 5060에 등록되지 않습니다.

3단계. 조직 2의 URI에 대한 SIP 경로 패턴을 생성하고 SIP 트렁크 포인트에 다음 이미지에 표시된 대로 Expressway-C에 할당합니다.

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

4단계. 이미지에 표시된 대로 CUCM을 가리키는 Expressway-C에 인접 영역을 생성합니다.

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 

5단계. 이미지에 표시된 대로 Expressway-C에 Traversal Client Zone(UC Traversal 아님)을 생성합니다.

EDIT 2016

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 ⓘ

6단계. 이미지에 표시된 대로 Expressway-E에 Traversal Server Zone(UC Traversal 아님)을 생성합니다.

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 ⓘ

7단계. Expressway-C에 DNS 영역을 생성합니다. 이 영역은 이미지에 표시된 대로 조직 2의 URI에 대한 DNS SRV 조회를 수행하는 데 사용됩니다.

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

H.323	
Mode	Off v i

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

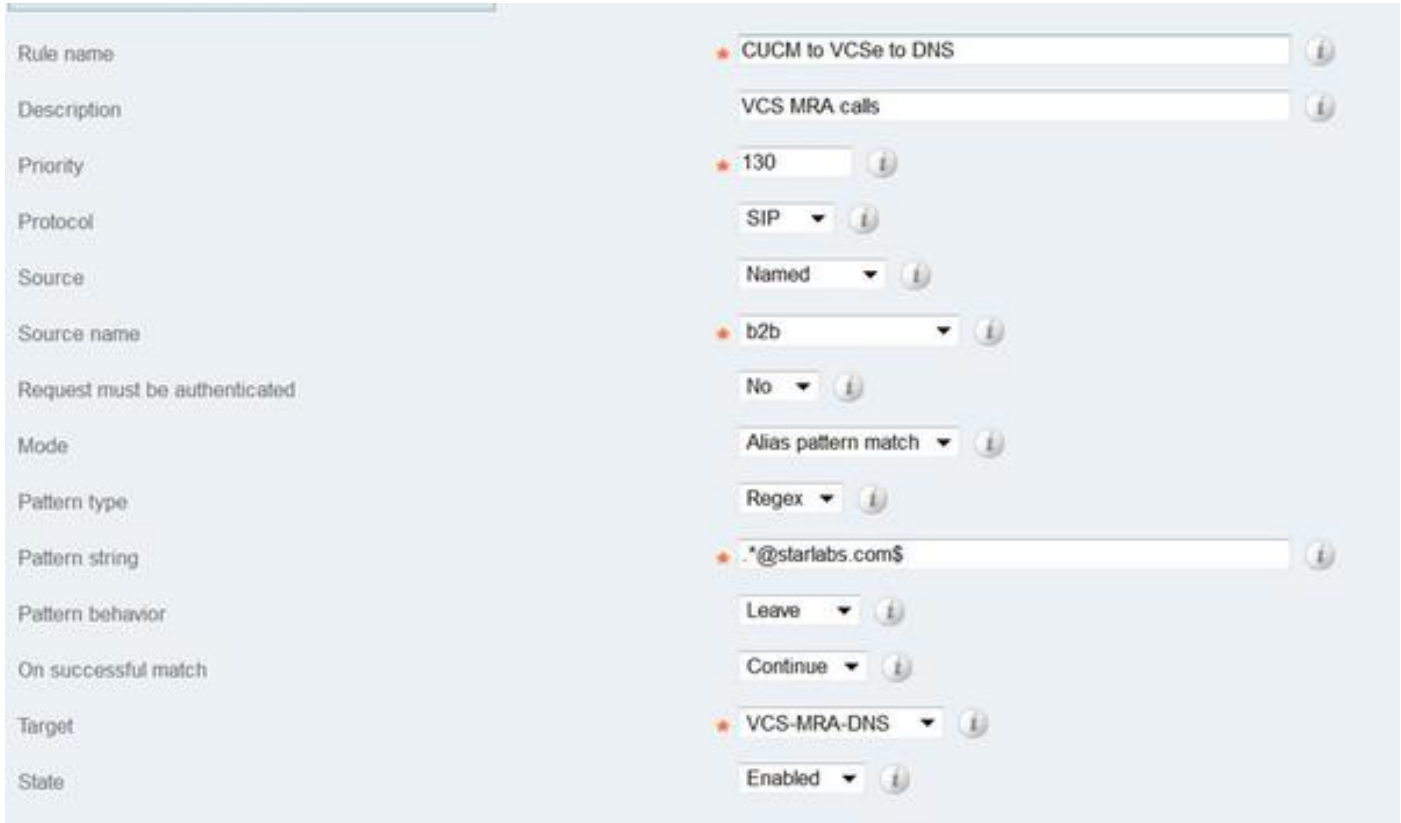
모든 영역이 만들어지면 라우팅을 수행할 수 있도록 Expressway C 및 E에서 검색 규칙을 정의해야 합니다.

8단계. Expressway-C의 검색 규칙은 이미지에 표시된 대로 URI starlabs.com에 대한 **SIP Invite**를 수행한 새 접근 영역에 Expressway-E로 전달하는 것입니다.

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

9단계. Expressway-E의 검색 규칙을 검색하여 URI starlabs.com에 대한 **SIP Invite**를 DNS 영역으

로 전달하려면 다음 이미지에 표시된 대로 통화가 Expressway-Evia traversal 영역에 도달하면 됩니다.



10단계. 통화가 DNS 영역에 도달하면 Expressway-C는 **_sips.tcp.starlabs.com**, **_sip.tcp.starlabs.com** 및 **_sip.udp.starlabs.com**에 대해 DNS SRV 조회를 수행합니다.

Exp-E 로그에서 다음과 같이 볼 수 있습니다.

```
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"
```

DNS SRV 조회에서 Exp-E는 조직 2에 연결하기 위한 다음 옵션의 IP 및 포트를 가져옵니다. 이 시나리오에서는 DNS SRV **_sip._tcp.starlabs.com**이 조직 2용 ASA의 공용 FQDN/IP 및 포트 5060으로 확인됩니다.

전체 아웃바운드 통화 흐름은

1. Jabber A는 **userB@starlabs.com**을 SIP URI로 다이얼합니다.
2. SIP Invite가 CUCM에 도달합니다(Exp-E → Exp-C를 통해).
3. CUCM은 **SIP Route Pattern**과 일치하는 숫자 분석을 수행합니다.
4. CUCM은 SIP 트렁크를 통해 통화를 Exp-C로 라우팅합니다.
5. Exp-C는 'CUCM Neighbor zone'에서 통화를 수신하고 'search rule'은 통화를 우리가 수행한

접근 영역으로 전달합니다.

- 이제 통화가 'traversal zone'을 통해 Exp-E에 도달하고 여기서 검색 규칙이 통화를 'DNS Zone'으로 전달합니다.
- DNS 영역에 도달하면 공용 DNS 서버에 대해 _sip._tcp.starlabs.com에 대한 DNS SRV 조회가 수행되며, 이는 조직 2에 도달하기 위한 다음 홉으로 확인됩니다.

Jabber B가 Jabber A를 호출할 때 조직 1의 구성

이제 Jabber B가 Jabber A를 호출할 때 조직 2에 SIP URI 통화를 조직 1로 라우팅하도록 구성된 자체 다이얼 플랜이 있다고 가정합니다. 조직 1의 CUCM으로 라우팅되는 수신 SIP INVITE를 가져오기 위해 필요한 변경 사항을 확인할 수 있습니다.

1단계. Expressway-E의 인바운드 검색 규칙 - 이미지에 표시된 대로 조직 2에서 Exp-C로 수신 SIP 초대를 fed.sollab1.com SIP URI 도메인에 보내기 위한 다음

The screenshot shows the configuration page for a search rule in Cisco Expressway. The rule is named 'VCSe to VCSc to CUCM' and is used for 'VCS MRA calls from outside'. The priority is set to 120, and the protocol is SIP. The source is set to 'Any', and 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	VCSe 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

2단계. Expressway-C의 인바운드 검색 규칙 - 이미지에 표시된 대로 Exp-E에서 CUCM으로 Incoming SIP 초대(fed.sollab1.com SIP URI 도메인에 대해)을 전송합니다.

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 ⓘ

전체 인바운드 통화 흐름은

1. userA@fed.sollab1.com용 Jabber B의 인바운드 SIP INVITE는 Exp-E를 적중합니다.
2. Exp-E의 검색 규칙은 'traversal zone'을 통해 통화를 Exp-C로 전달합니다.
3. Exp-C의 검색 규칙은 'CUCM 인접 영역'을 통해 통화를 CUCM 클러스터로 전달합니다.
4. CUCM은 MRA를 통해 등록된 Jabber A에 SIP Invite를 보냅니다(Exp-C → Exp-E 사용).

참고:B2B 통화가 작동하려면 Expressway-C 및 Expressway-E에서 리치 미디어 라이선스가 필요합니다.

참고:고객이 방화벽에 올바른 포트를 열었는지 확인합니다.