

Chamadas URI do Jabber SIP por MRA

Contents

[Introduction](#)

[Cenário](#)

[Hipóteses levantadas](#)

[Configuração na Organização 1 quando o Jabber A chama o Jabber B](#)

[O fluxo geral de chamada de saída torna-se](#)

[Configuração na Organização 1 quando o Jabber B chama o Jabber A](#)

[O fluxo geral da chamada de entrada torna-se](#)

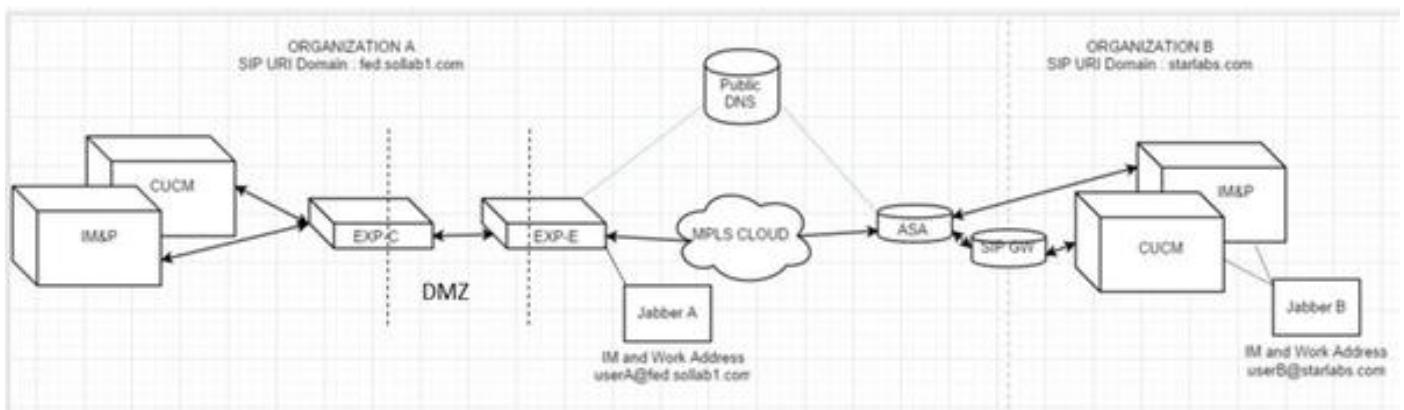
Introduction

Este documento descreve a configuração envolvida no Cisco Unified Communications Manager (CUCM) e no Expressway C e E para que o Jabber possa chamar o URI (Uniform Resource Identifier) do SIP (Session Initiation Protocol) de outro usuário de uma organização diferente quando conectado por MRA (Mobile Remote Access). O mesmo no contexto do Expressway também é chamado de fluxo de chamada B2B.

Cenário

Suponha um cenário em que a Organização 1 implanta MRA e a Organização 2 não. Para a empresa 2, o perímetro termina com um Adaptive Security Appliance (ASA), além do qual há o CUBE integrado ao cluster CUCM da Organização 2.

Como mostrado na imagem, o Jabber A pode ser conectado por MRA ou internamente, mas a configuração permanece a mesma no CUCM, Expressway C e E, para a Organização 1.



Hipóteses levantadas

Você pode supor que o usuário Jabber A e o usuário Jabber B podem trocar mensagens

instantâneas e presença pela federação XMPP (Extensible Messaging and Presence Protocol), e seus endereços IM também são URIs SIP de trabalho.

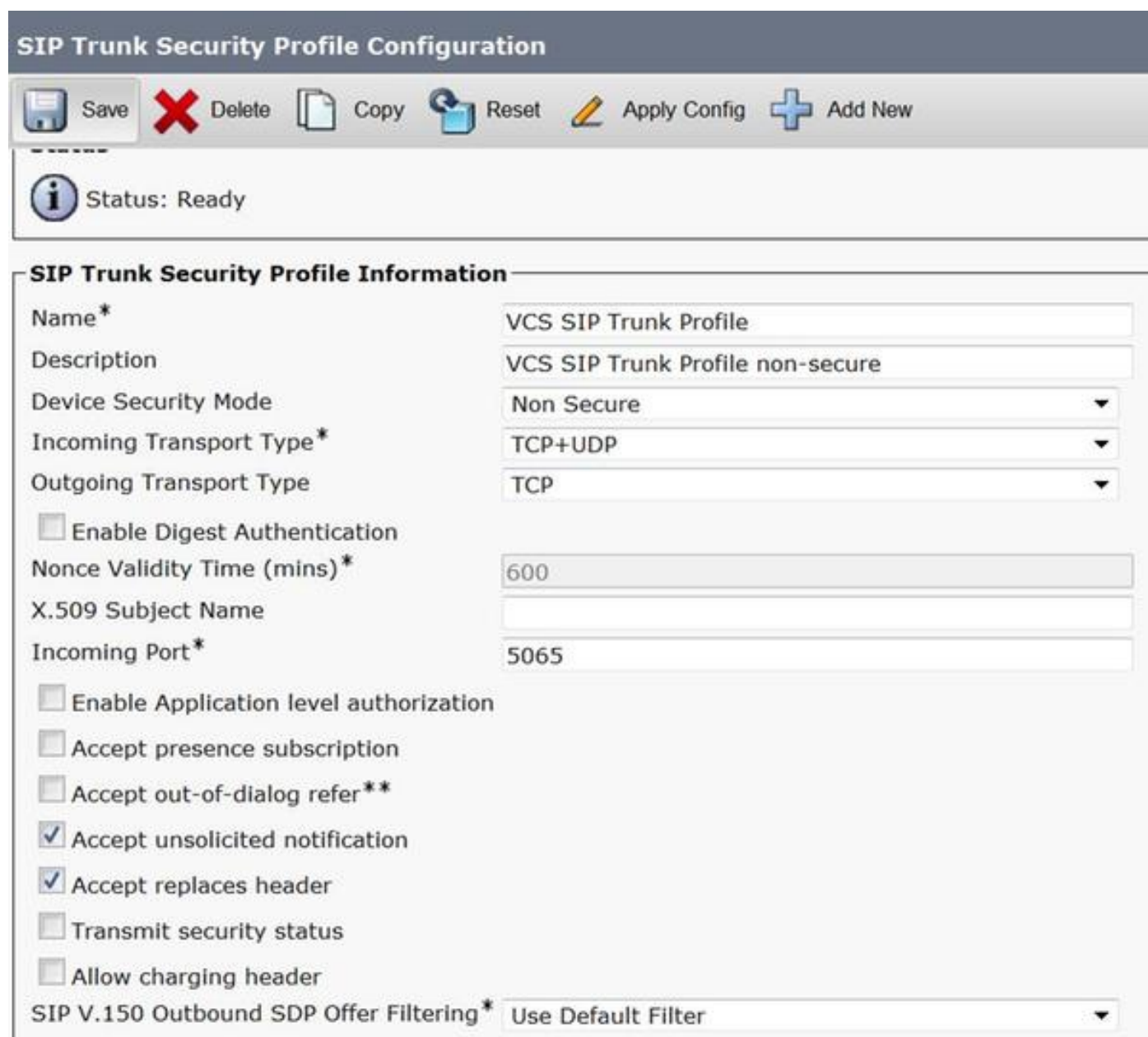
Além disso, o Jabber A e o Jabber B podem discar via URI SIP internamente, dentro de suas respectivas organizações, com êxito.

No cenário acima, você supõe que a Organização 2 tenha o CUCM como um servidor de controle de chamadas. No entanto, também pode ser um servidor de controle de chamadas de um fornecedor diferente.

A consciência da versão é necessária durante a integração do CUCM, Jabber, VCS para MRA.

Configuração na Organização 1 quando o Jabber A chama o Jabber B

Etapa 1. Crie um novo perfil de segurança de tronco SIP, que tenha uma porta de escuta de 5065, como mostrado na imagem:



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

Etapa 2. Crie um tronco SIP apontando para o ExpressWay-C e atribua o perfil de segurança do tronco SIP, como mostrado na imagem:

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


Note: Um novo perfil de segurança de tronco é criado e é ouvido na porta 5065. Ele é atribuído a esse novo tronco SIP que aponta para o Expressway-C porque o Expressway-C já está configurado para enviar registros não seguros do Jabber no 5060 para o CUCM quando o usuário do Jabber faz login via MRA. Se você usa o perfil de segurança de tronco padrão, o jabber conectado via MRA não consegue se registrar na porta 5060 do CUCM.

Etapa 3. Crie o padrão de rota SIP para o URI da Organização 2 e atribua-o ao ponto de tronco SIP para o Expressway-C, como mostrado na imagem:

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

Etapa 4. Crie uma Zona de Vizinho no Expressway-C apontando para CUCM, como mostrado na imagem:

The image shows a configuration interface for Expressway-C, 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

Etapa 5. Crie uma Zona de Cliente Transversal no Expressway-C (Não um Transversal de UC), como mostrado na imagem:

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 ▼ ⓘ

Etapa 6. Crie uma zona de servidor transversal no Expressway-E (não um caminho de UC), como mostrado na imagem:

Edit zone

Type	Traversal server
Hop count	15 <input type="text"/>

Connection credentials

Username	cisco <input type="text"/>
Password	Add/Edit local authentication database

H.323

Mode	Off <input type="text"/>
------	--------------------------

SIP

Mode	On <input type="text"/>
Port	7003 <input type="text"/>
Transport	TCP <input type="text"/>
Accept proxied registrations	Allow <input type="text"/>
Media encryption mode	Auto <input type="text"/>
ICE support	Off <input type="text"/>
...	Off <input type="text"/>

Passo 7. Crie uma zona DNS no Expressway-C, que seria usada para fazer uma pesquisa de DNS SRV para o URI da Organização 2, como mostrado na imagem:

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

Depois que todas as zonas forem criadas, você precisará definir as regras de pesquisa no Expressway C e E para que o roteamento possa ocorrer.

Etapa 8. A regra de pesquisa no Expressway-C é encaminhar o **convite SIP** destinado a URI starlabs.com para Expressway-E , na nova zona de passagem que você fez, como mostrado na imagem:

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

Etapa 9. Regra de pesquisa no Expressway-E , para encaminhar o **convite SIP** destinado a URI starlabs.com para DNS ZONE , uma vez que a chamada atinja o Expressway-Evia na zona de passagem, que você fez, como mostrado na imagem:

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

Etapa 10. Quando a chamada atinge a zona DNS , o Expressway-C faz uma pesquisa SRV DNS para **_sips.tcp.starlabs.com**, **_sip._tcp.starlabs.com** e **_sip._udp.starlabs.com** contra o servidor DNS público.

Nos registros do Exp-E, você pode ver isso como:

```
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"
```

Na pesquisa de SRV de DNS, o Exp-E obtém o IP e a porta do próximo salto para acessar a Organização 2. Neste cenário, o DNS SRV **_sip._tcp.starlabs.com** resolve para o FQDN/IP público e a porta 5060 do ASA para a Organização 2.

O fluxo geral de chamada de saída torna-se

1. O Jabber A disca **userB@starlabs.com** como URI SIP.
2. O convite do SIP alcança o CUCM (via Exp-E → Exp-C).
3. O CUCM faz a análise de dígitos que corresponde ao **padrão de rota SIP**.
4. O CUCM roteia a chamada para o Exp-C por Tronco SIP.

5. O Exp-C recebe a chamada na 'zona vizinha do CUCM' e a 'regra de pesquisa' encaminha a chamada para a zona de passagem que fizemos.
6. A chamada agora chega ao Exp-E por meio da 'zona de passagem' e a regra de pesquisa aqui encaminha a chamada para 'Zona de DNS'.
7. Depois de alcançar a zona DNS, acontece a pesquisa SRV DNS para `_sip._tcp.starlabs.com` em relação ao servidor DNS público, que resolve para o próximo salto para acessar a Organização 2.

Configuração na Organização 1 quando o Jabber B chama o Jabber A

Agora suponha que a Organização 2 tenha seu próprio plano de discagem configurado para rotear uma chamada URI SIP para a Organização 1, quando o Jabber B chamar o Jabber A. Vamos ver as alterações necessárias para obter o CONVITE SIP de entrada, roteado para o CUCM da Organização 1.

Etapa 1. Regra de Pesquisa de Entrada no Expressway-E, para enviar um Convite SIP de Entrada da Organização 2 para o Exp-C, para domínio URI **alimentado.sollab1.com**, como mostrado na imagem:

The image shows a configuration interface for a rule. The rule name is 'VCSe to VCSc to CUCM' and the description is 'VCS MRA calls from outside'. The priority is set to 120, the protocol is SIP, and the source is Any. The request must be authenticated is set to No. The mode is Alias pattern match, the pattern type is Regex, and the pattern string is `.*@fed.sollab1.com$`. The pattern behavior is Leave, and the on successful match action is Continue. The target is b2b, and the state 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

Etapa 2. Regra de pesquisa de entrada no Expressway-C, para enviar um convite SIP de entrada do Exp-E para o CUCM, para domínio URI **alimentado.sollab1.com**, como mostrado na imagem:

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 ⓘ

O fluxo geral da chamada de entrada torna-se

1. CONVITE SIP de entrada do Jabber B para **userA@fed.sollab1.com** atinge o Exp-E.
2. A regra de pesquisa no Exp-E encaminha a chamada para o Exp-C, por meio da 'zona de passagem'.
3. A regra de pesquisa no Exp-C encaminha a chamada para o cluster CUCM por meio da 'Zona de vizinhos CUCM'.
4. O CUCM envia o convite SIP para o Jabber A registrado no MRA (via Exp-C → Exp-E).

Note: Licenças de mídia avançada são necessárias para que as chamadas do Expressway-C e do Expressway-E para B2B funcionem.

Note: Certifique-se de que o cliente tenha aberto as portas corretas no firewall.