Jabber SIP URI calls over MRA

Contents

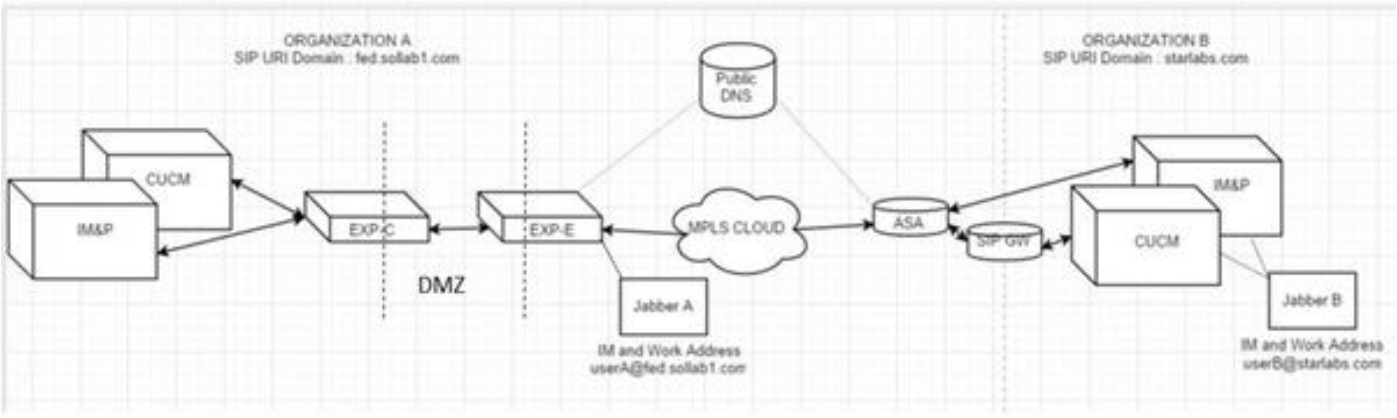
Introduction

This document describes the configuration involved on Cisco Unified Communications Manager (CUCM) and Expressway C and E so that jabber can call the Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) of an another user from a different organization when connected over Mobile Remote Access (MRA). The same in Expressway's context is also called B2B call flow.

Scenario

Assume a scenario wherein Organization 1 deploys MRA and Organization 2 does not. For organization 2, the perimeter ends with an Adaptive Security Appliance (ASA), beyond which there is CUBE which is integrated with CUCM cluster of Organization 2.

As shown in the image, Jabber A can be connected over MRA or internally, but the configuration remains the same on CUCM, Expressway C and E, for Organization 1.



Assumptions Made

You can assume that Jabber A user and Jabber B user are able to exchange IM and presence

over Extensible Messaging and Presence Protocol (XMPP) federation, and their IM addresses are also their Work SIP URIs.

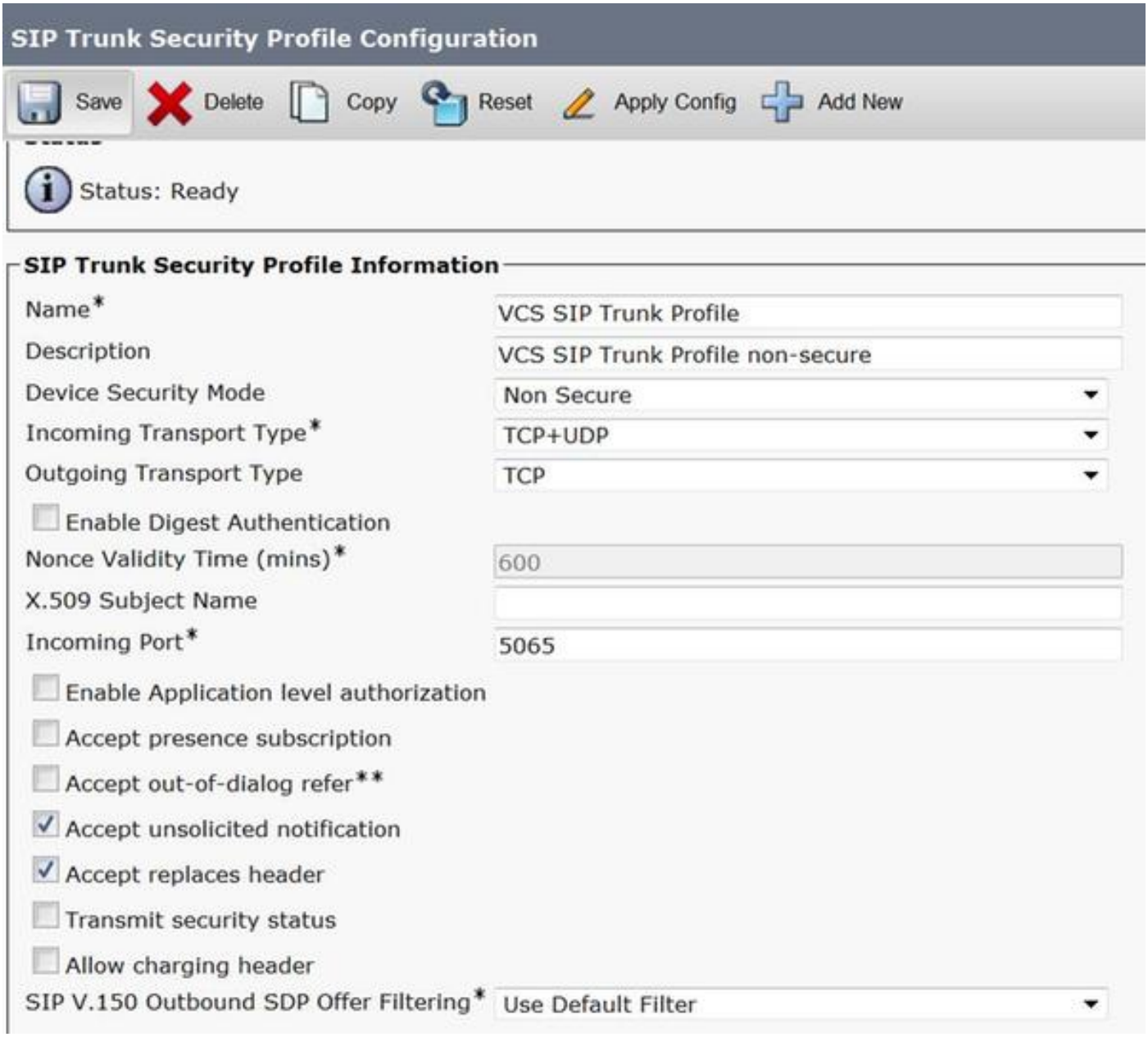
Also, Jabber A and Jabber B are able to dial via SIP URI internally, inside their respective organizations, successfully.

In the above scenario, you assume that Organization 2 has CUCM as a call control server. However, it can be a call control server from a different vendor as well.

Awareness of the version is needed while integrating CUCM, Jabber, VCS for MRA.

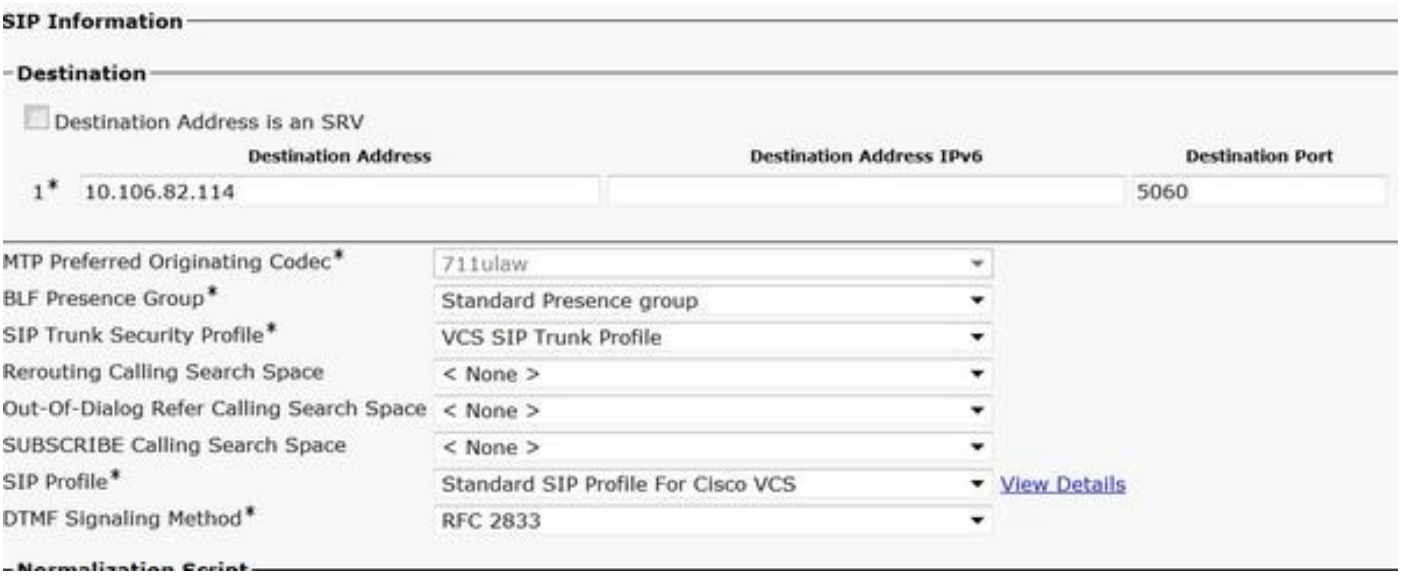
Configuration on Organization 1 when Jabber A calls Jabber B

Step 1. Create a New SIP Trunk Security profile, which has a listening port of 5065, as shown in the image:



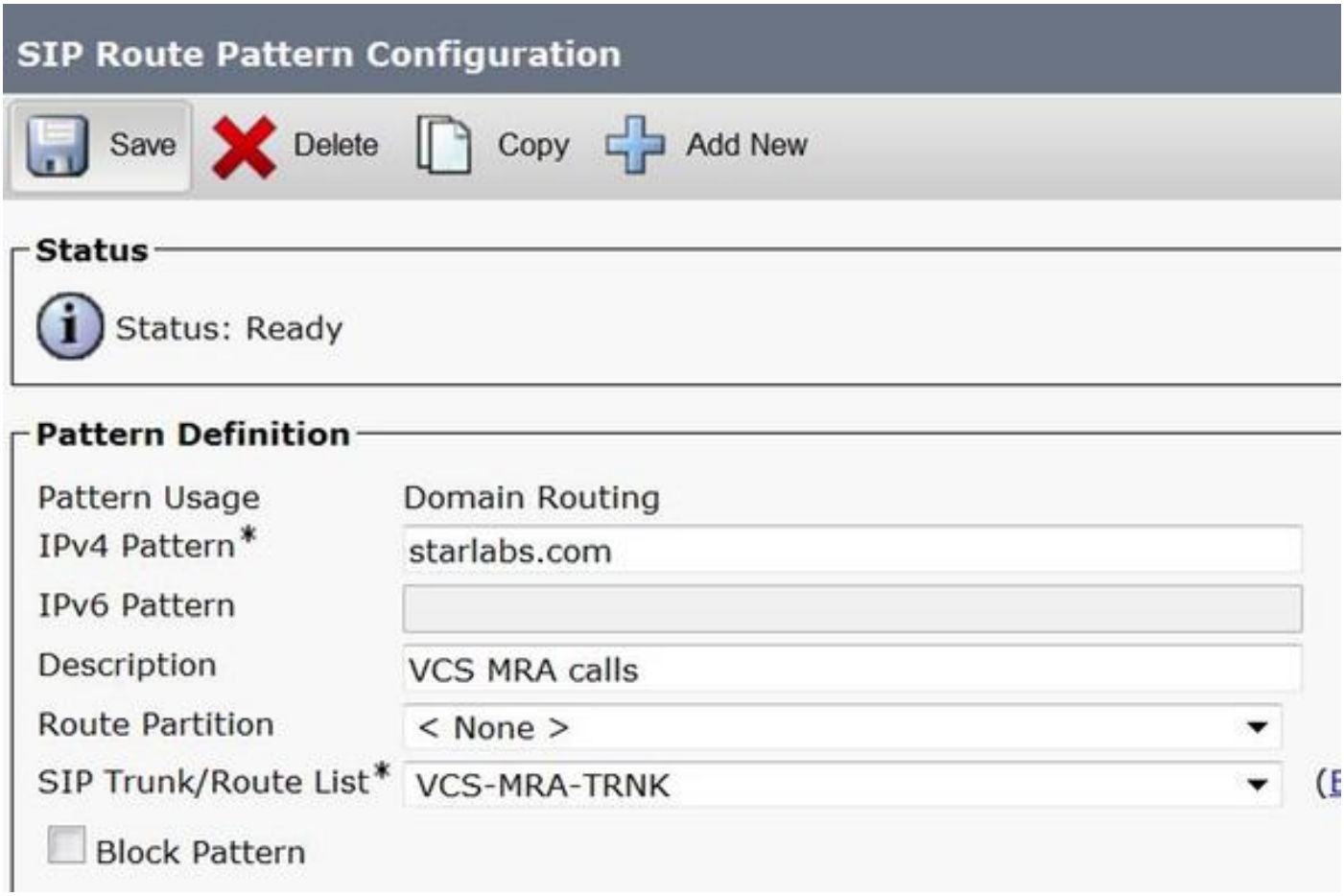
Step 2. Create a SIP Trunk pointing to ExpressWay-C and assign the SIP Trunk Security profile,

as shown in the image:

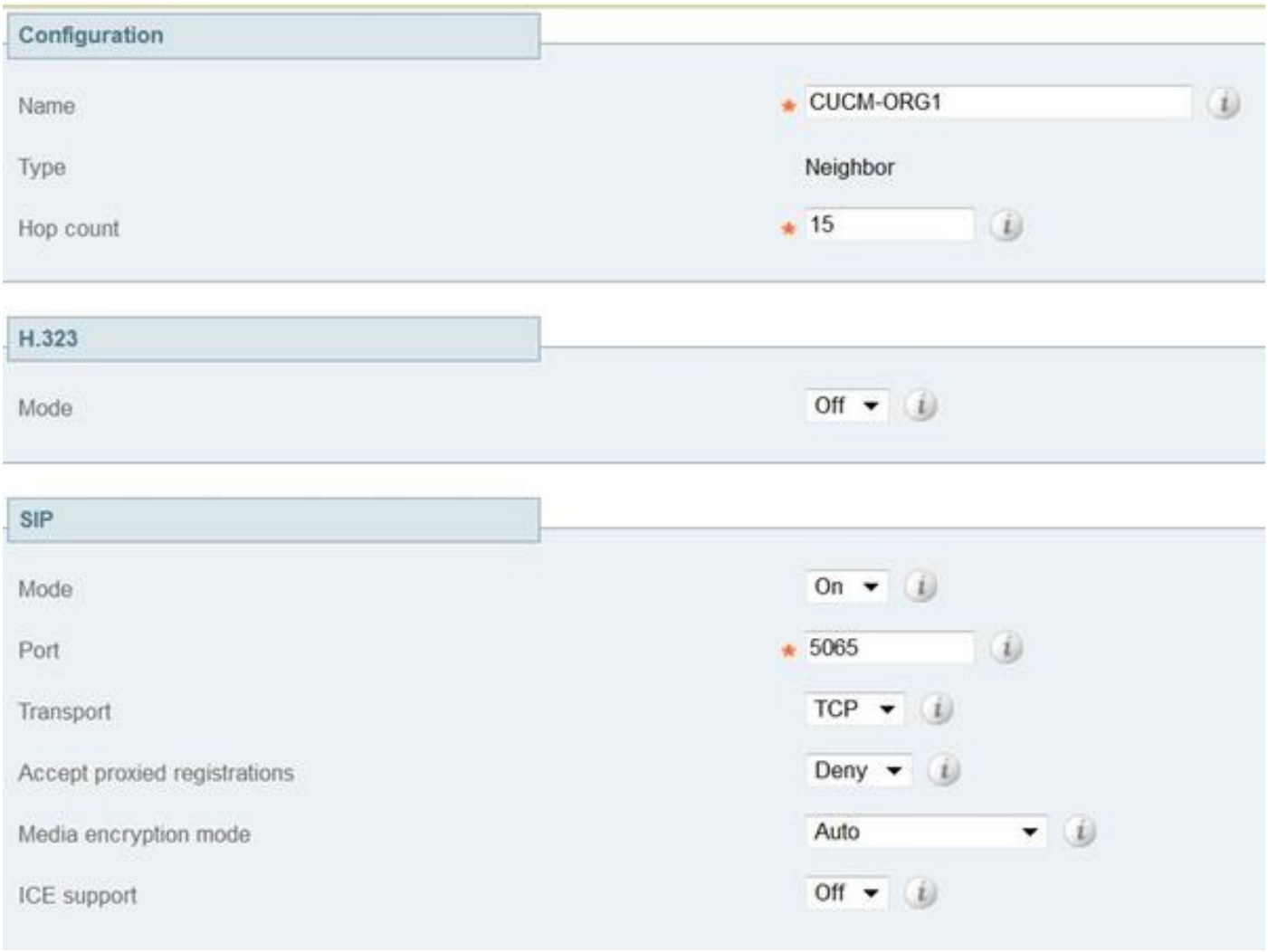


Note: A new Trunk Security profile is created which listens on 5065 port. It is assigned to this new SIP trunk pointing to Expressway-C because Expressway-C is already configured to send Jabber Un-secure registrations on 5060 to CUCM when Jabber user logs in via MRA. If you use the default Trunk Security profile, then jabber logged in via MRA fails to register on port 5060 of CUCM.

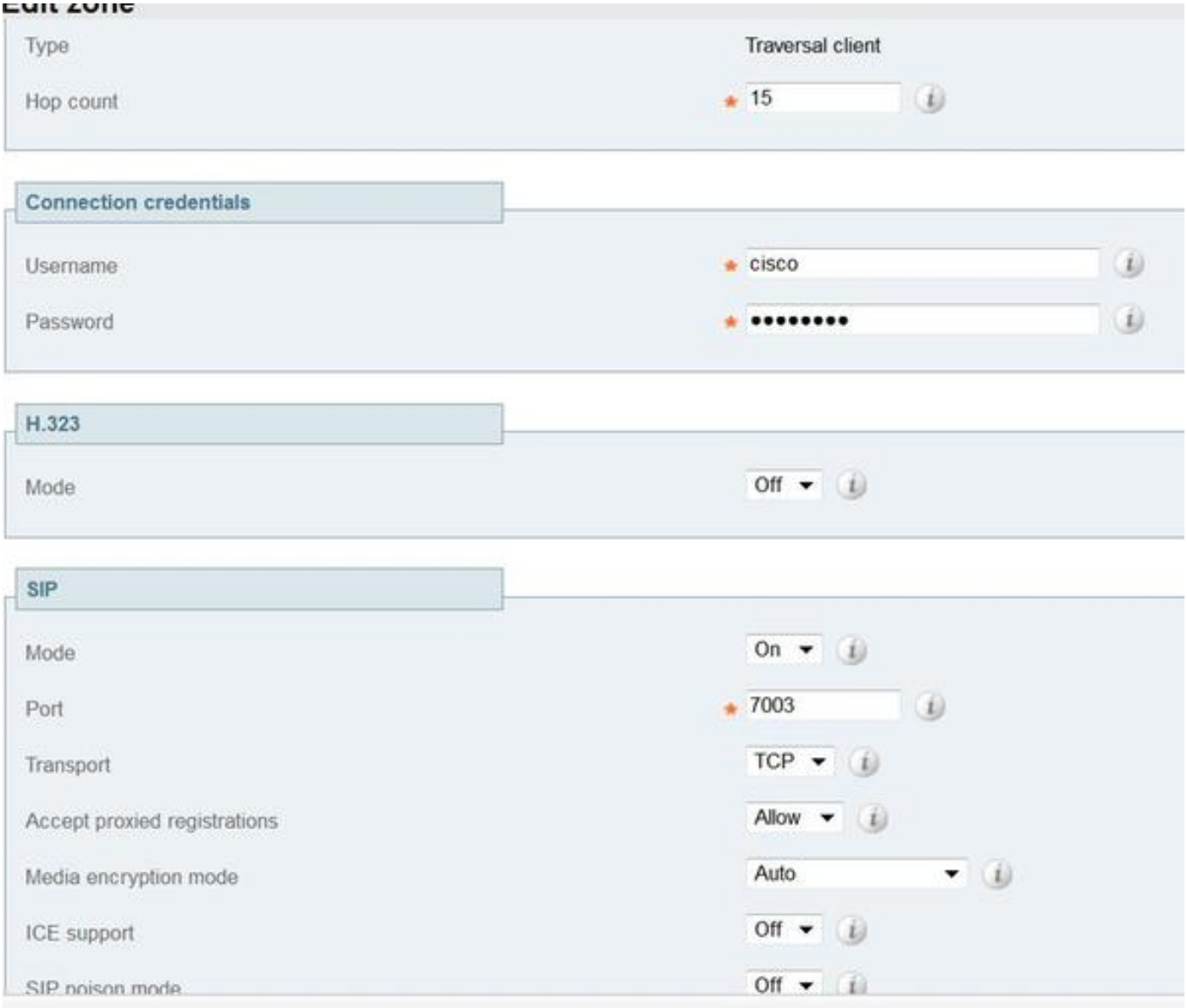
Step 3. Create SIP Route Pattern for the URI of Organization 2 and assign that to SIP Trunk point to Expressway-C, as shown in the image:



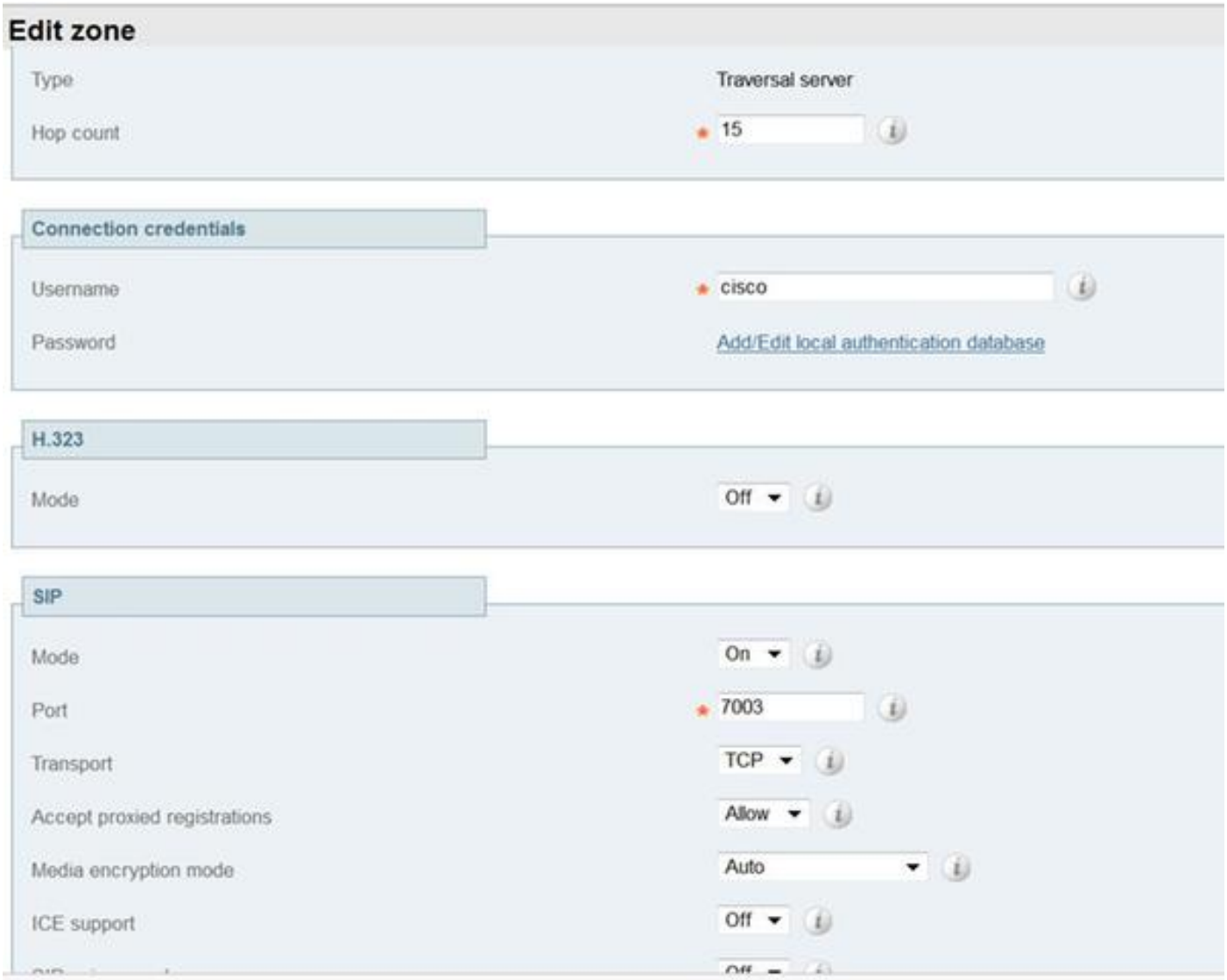
Step 4. Create a Neighbor Zone on Expressway-C pointing to CUCM, as shown in the image:



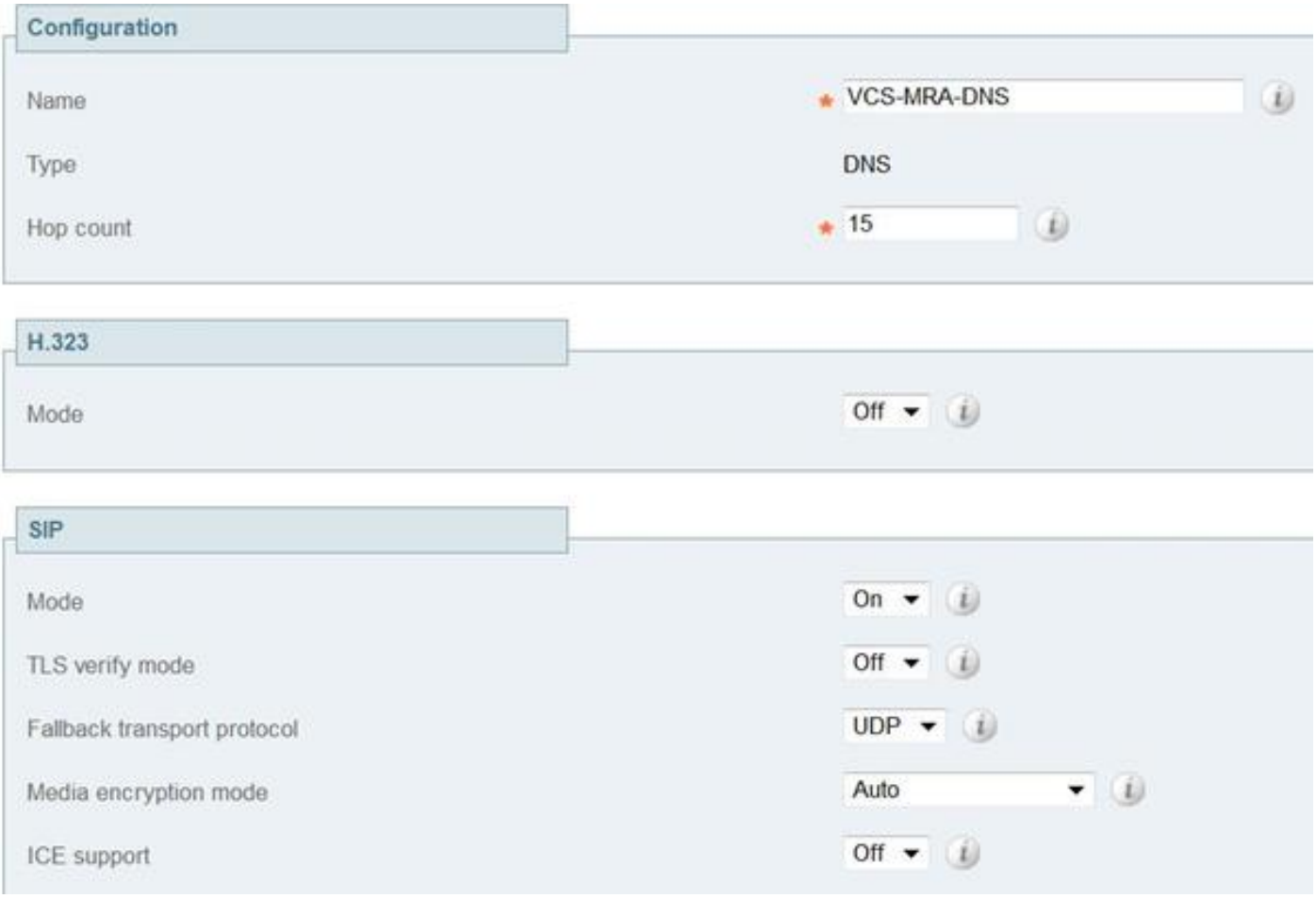
Step 5. Create a Traversal Client Zone on the Expressway-C (Not a UC Traversal)**,** as shown in the image:



Step 6. Create a Traversal Server Zone on the Expressway-E (Not a UC Traversal), as shown in the image:

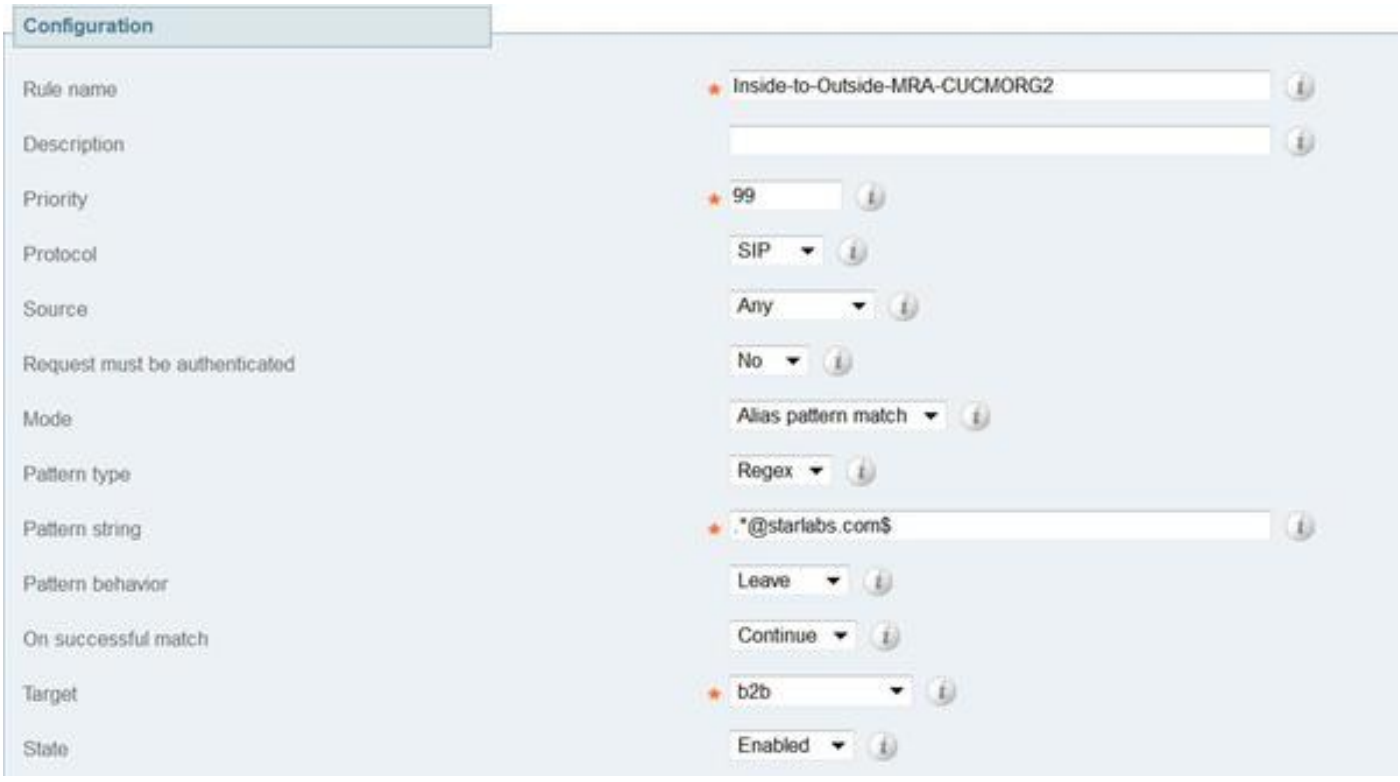


Step 7. Create a DNS Zone on Expressway-C, which would be used to do a DNS SRV lookup for Organization 2's URI, as shown in the image:



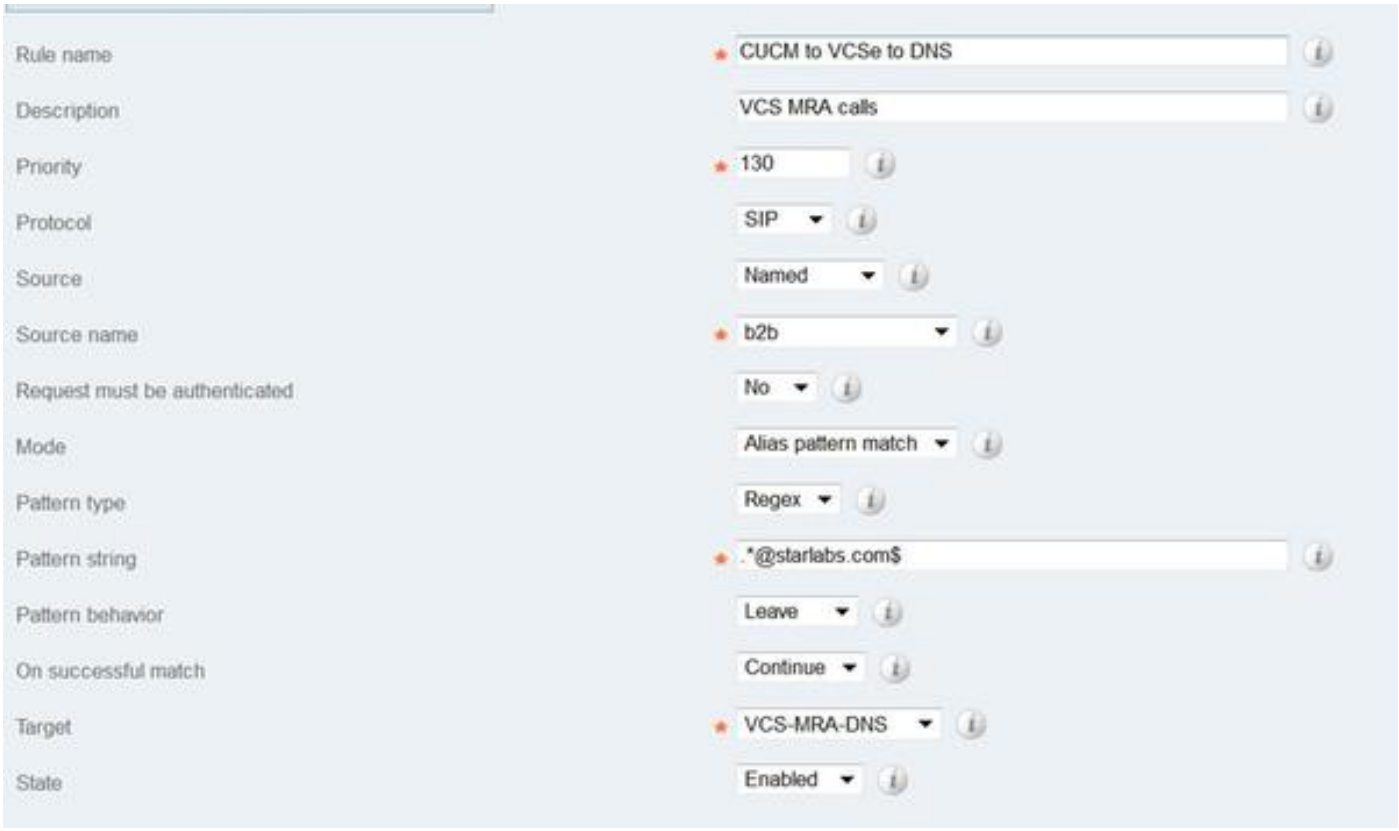
Once all the zones are made, you need to define Search Rules on Expressway C and E so that the routing can take place.

Step 8. Search Rule on Expressway-C is to forward the **SIP Invite** meant for URI starlabs.com to Expressway-E , on the new traversal zone that you have made, as shown in the image:



Step 9. Search Rule on Expressway-E , to forward the **SIP Invite** meant for URI starlabs.com to

DNS ZONE , once the call reaches Expressway-Evia the traversal zone, that you have made, as shown in the image:



Step 10. Once the Call hits the DNS Zone , Expressway-C does a DNS SRV Lookup for **_sips.tcp.starlabs.com**, **_sip._tcp.starlabs.com** and **_sip._udp.starlabs.com** against the Public DNS Server.

In the Exp-E logs , you can see this as:

```
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"
```

From the DNS SRV lookup , Exp-E get the IP and port for the next hop, for reaching the Organization 2. In this scenario the DNS SRV **_sip._tcp.starlabs.com** resolves to the public FQDN/IP & port 5060 ,of the ASA for Organization 2.

Overall Oubound Call flow becomes

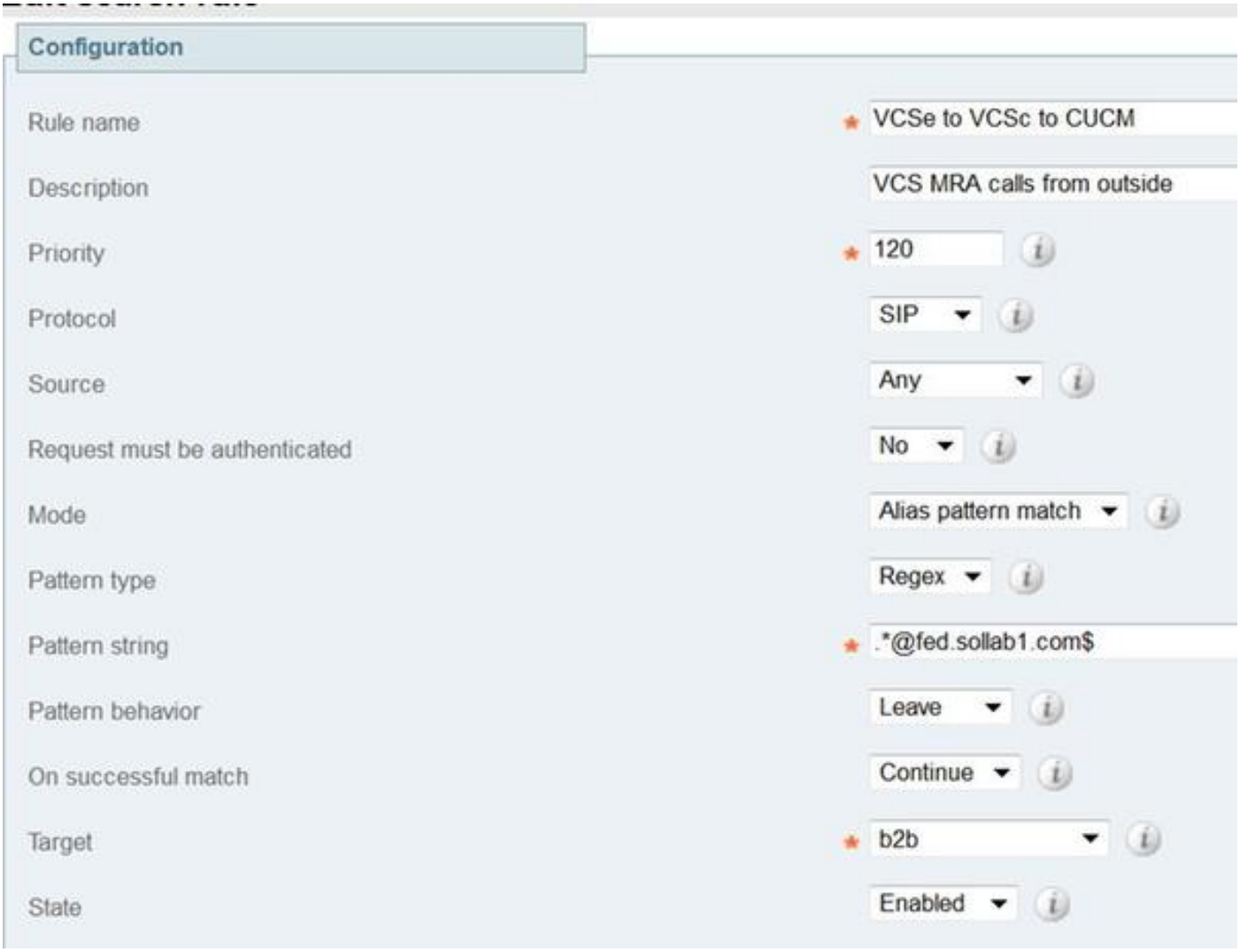
1. Jabber A dials **userB@starlabs.com** as SIP URI.
2. SIP Invite reaches CUCM (via Exp-E --> Exp-C).
3. CUCM does digit Analysis which matches **SIP Route Pattern**.
4. CUCM route the call to Exp-C via SIP Trunk.
5. Exp-C receives the call on the 'CUCM Neighbor zone' , and the 'search rule' forwards the call

to the traversal zone we made.
6. Call now reaches the Exp-E via the 'traversal zone' and the search rule here forwards the call to 'DNS Zone'.
7. Once reaching the DNS Zone, DNS SRV lookup for _sip._tcp.starlabs.com against the Public DNS Server happens, which resolves to the next hop for reaching Organization 2.

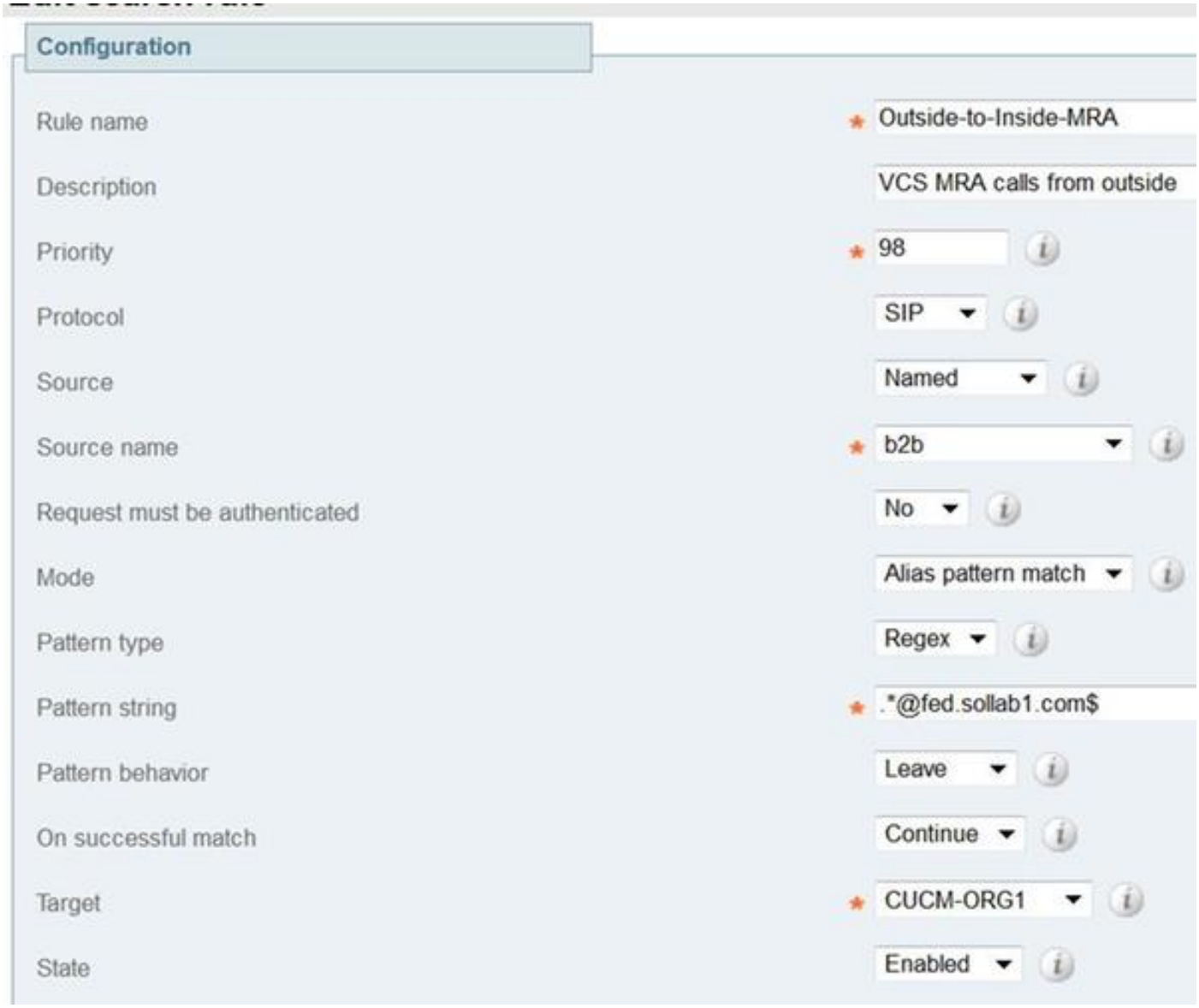
Configuration on Organization 1 when Jabber B calls Jabber A

Now assume, Organization 2 has its own dial plan configured to route a SIP URI call to Organization 1, when jabber B calls Jabber A. Lets see what changes you need, to get the incoming SIP INVITE , routed to CUCM of Organization 1.

Step 1. Inbound Search Rule on Expressway-E, for sending an Incoming SIP Invite from Organization 2 to Exp-C, for **fed.sollab1.com** SIP URI domain, as shown in the image:



Step 2. Inbound Search Rule on Expressway-C, for sending an Incoming SIP invite from Exp-E to CUCM, for **fed.sollab1.com** SIP URI domain, as shown in the image:



Overall Inbound Call flow becomes

1. Inbound SIP INVITE from Jabber B for **userA@fed.sollab1.com** hits Exp-E.
2. Search Rule on Exp-E forwards the call to Exp-C,via the 'traversal zone'.
3. Search Rule on Exp-C , forwards the Call to CUCM Cluster via the 'CUCM Neighbor Zone'.
4. CUCM sends the SIP Invite to Jabber A registered over MRA (via Exp-C --> Exp-E).

Note: Rich Media Licenses are needed on both Expresssway-C and Expresssway-E for B2B calls to work.

Note: Ensure that the customer had the correct ports opened up on the firewall.