MRA phone services failing due to source IP translation over NAT reflection (single NIC configuration with static NAT enabled)

Contents

Introduction
Prerequisites
Components Used
Background Information
Problem
Network Diagram
Details
Evidence in Diagnostic Logs
Solution
Disable the source IP port translation on the firewall
Move to a dual NIC configuration
Related Information

Introduction

This document describes how to troubleshoot phone services failure over MRA caused by source IP translation over NAT reflection, with Expressway-E single-NIC with Static NAT configuration.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- NAT (Network Address Translation)
- SIP (Session Initiation Protocol)
- Cisco Video Communication Server (VCS) or Expressway basic configuration
- Mobile and Remote Access (MRA) over Expressway or VCS

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

> **Note**: Through the entire document, Expressway devices are referred as Expressway-E and Expressway-C. However, the same configuration applies to Video Communication Server

(VCS) Expressway and VCS Control devices.

Background Information

This document covers a schenario in which Mobile and Remote Access has been deployed on Expressway with Expressway-E using a single NIC and Static NAT address (described as 3-port Firewall DMZ Using Single Expressway-E LAN Interface, as described in the Expressway Basic Configuration Guide). MRA users are able to log in successfully, but do not have access to phone services.

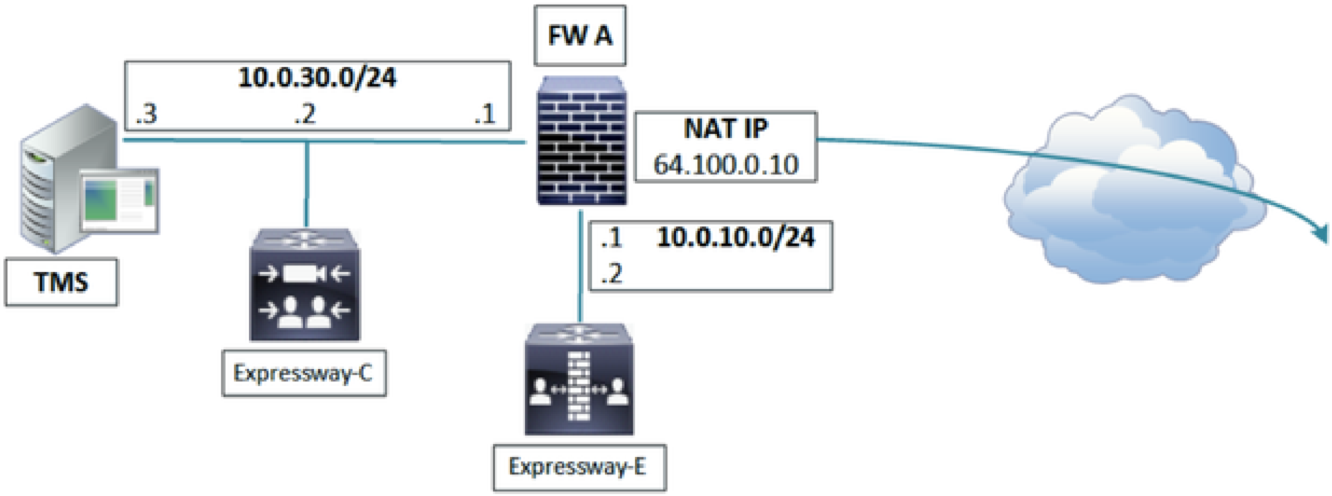
The SIP REGISTER message from external client is received by Expressway-E successfully on port 5061.
Expressway-E then creates a SIP SERVICE message towards Expressway-C. This request results in a 408 Request Timeout.

Problem

Phone services fail because the SIP REGISTER message does not go through to the Cisco Unified Communications Manager (CUCM or Call Manager). Expressway-E and Expressway-C are not able to exchange their certificates properly using the SIP SERVICE message exchange. The SIP SERVICE messages only get a 408 Request Timeout as response from the Expressway-C. As the SIP SERVICE message is not successful, the Expressway-E does not forward the SIP REGISTER message to the Expressway-C.
This is caused by the fact that the firewall between Expressway-C and Expressway-E does source IP (and port) translation for messages from the Expressway-C to the Expressway-E. This results in the Expressway-C routing those SIP SERVICE messages incorrectly towards that translated address, instead of its own local address. In a successful scenario, the Expressway-C processes the SIP SERVICE message itself. (The SIP SERVICE message between Expressway-E and Expressway-C is used to check certificates and therefore only seen at the beginning of a traversal zone setup, or upon first registration over MRA.)

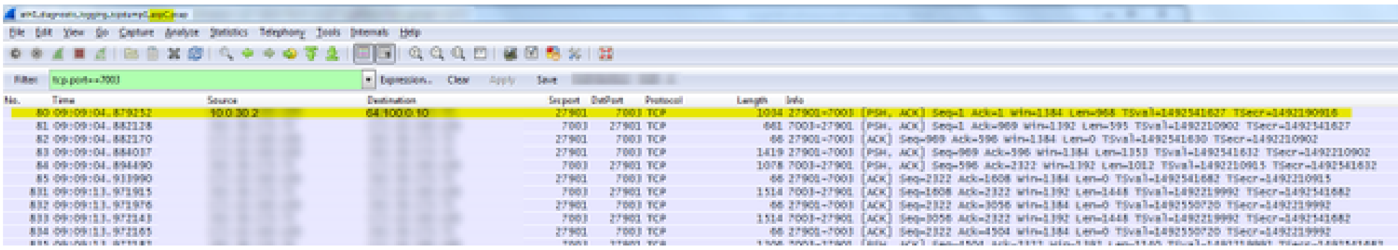
Network Diagram

The following image provides an example of a network diagram, which is used as a reference throughout this document:



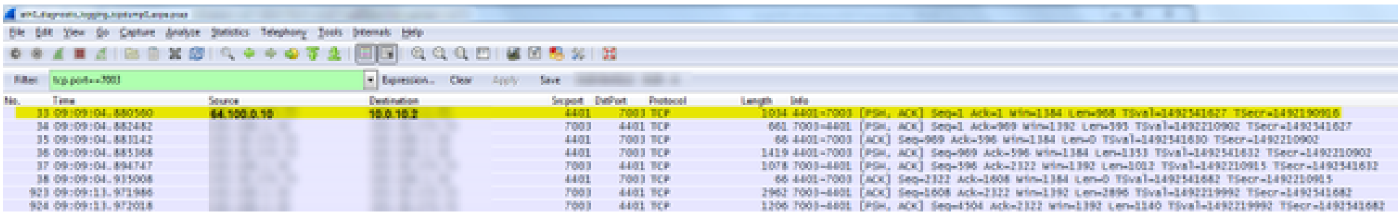
Details

From the Expressway-C packet captures, you can see that the Expressway-C (10.0.30.2) connects successfully to the Expressway-E static NAT public IP address (64.100.0.10) on port 7003. (Notice that the source port is 27901 on the Expressway-C):


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port==7003
Expression... Clear Apply Save

```
No.  Time             Source     Destination  Srcport DstPort Protocol Length Info
 80 09:09:04.879252  10.0.30.2  64.100.0.10   27901   7003 TCP   1034 27901→7003 [PSH, ACK] Seq=1 Ack=1 Win=1384 Len=968 TSval=1492541627 TSecr=1492190916
 81 09:09:04.882128                            7003  27901 TCP    661 7003→27901 [PSH, ACK] Seq=1 Ack=969 Win=1392 Len=595 TSval=1492210902 TSecr=1492541627
 82 09:09:04.882170                           27901   7003 TCP     66 27901→7003 [ACK] Seq=969 Ack=596 Win=1384 Len=0 TSval=1492541630 TSecr=1492210902
 83 09:09:04.884037                           27901   7003 TCP   1419 27901→7003 [PSH, ACK] Seq=969 Ack=596 Win=1384 Len=1353 TSval=1492541632 TSecr=1492210902
 84 09:09:04.894490                            7003  27901 TCP   1078 7003→27901 [PSH, ACK] Seq=596 Ack=2322 Win=1392 Len=1012 TSval=1492210915 TSecr=1492541632
 85 09:09:04.933990                           27901   7003 TCP     66 27901→7003 [ACK] Seq=2322 Ack=1608 Win=1384 Len=0 TSval=1492541682 TSecr=1492210915
831 09:09:13.971915                            7003  27901 TCP   1514 7003→27901 [ACK] Seq=1608 Ack=2322 Win=1392 Len=1448 TSval=1492219992 TSecr=1492541682
832 09:09:13.971976                           27901   7003 TCP     66 27901→7003 [ACK] Seq=2322 Ack=3056 Win=1384 Len=0 TSval=1492550720 TSecr=1492219992
833 09:09:13.972143                            7003  27901 TCP   1514 7003→27901 [ACK] Seq=3056 Ack=2322 Win=1392 Len=1448 TSval=1492219992 TSecr=1492541682
834 09:09:13.972165                           27901   7003 TCP     66 27901→7003 [ACK] Seq=2322 Ack=4504 Win=1384 Len=0 TSval=1492550720 TSecr=1492219992
835 09:09:13.972187                            7003  27901 TCP   1206 7003→27901 [PSH, ACK] Seq=4504 Ack=2322 Win=1392 Len=1140 TSval=1492219992 TSecr=1492541682
```

In packet captures of the Expressway-E you can see that the connection comes from 64.100.0.10 on port 4401 (which is its own static NAT public IP address) with destination 10.0.10.2 and port 7003:


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port==7003
Expression... Clear Apply Save

```
No.  Time             Source       Destination  Srcport DstPort Protocol Length Info
 33 09:09:04.880560  64.100.0.10  10.0.10.2     4401   7003 TCP   1034 4401→7003 [PSH, ACK] Seq=1 Ack=1 Win=1384 Len=968 TSval=1492541627 TSecr=1492190916
 34 09:09:04.882482                             7003   4401 TCP    661 7003→4401 [PSH, ACK] Seq=1 Ack=969 Win=1392 Len=595 TSval=1492210902 TSecr=1492541627
 35 09:09:04.883142                             4401   7003 TCP     66 4401→7003 [ACK] Seq=969 Ack=596 Win=1384 Len=0 TSval=1492541630 TSecr=1492210902
 36 09:09:04.885368                             4401   7003 TCP   1419 4401→7003 [PSH, ACK] Seq=969 Ack=596 Win=1384 Len=1353 TSval=1492541632 TSecr=1492210902
 37 09:09:04.894747                             7003   4401 TCP   1078 7003→4401 [PSH, ACK] Seq=596 Ack=2322 Win=1392 Len=1012 TSval=1492210915 TSecr=1492541632
 38 09:09:04.935008                             4401   7003 TCP     66 4401→7003 [ACK] Seq=2322 Ack=1608 Win=1384 Len=0 TSval=1492541682 TSecr=1492210915
923 09:09:13.971986                             7003   4401 TCP   2962 7003→4401 [ACK] Seq=1608 Ack=2322 Win=1392 Len=2896 TSval=1492219992 TSecr=1492541682
924 09:09:13.972018                             7003   4401 TCP   1206 7003→4401 [PSH, ACK] Seq=4504 Ack=2322 Win=1392 Len=1140 TSval=1492219992 TSecr=1492541682
```

These are the perspectives of the connection between Expressway-C and E:

Expressway-C : 10.0.30.2:27901 <-> 64.100.0.10:7003
Expressway-E : 64.100.0.10:4401 <-> 10.0.10.2:7003

This indicates that the firewall between Expressway-C and Expressway-E is doing source IP and port translation on those messages.
If you have a look at the flow of SIP communication on Expressway-E, you can see it gets the SIP REGISTER from the MRA client device, then Expressway-E generates a SIP SERVICE message to exchange its certificates with the Expressway-C, but this results in a 408 Request Timeout.

Evidence in Diagnostic Logs

Notice that the Route header of this SIP SERVICE message (sent from Expressway-E to Expressway-C) contains the IP and port of the NAT address (64.100.0.10:4401).
When this message arrives at the Expressway-C, Expressway-C tries to route the message based on that Route header, towards 64.100.0.10:4401. This fails as it is not able to make a connection to this address, as this address is on the Expressway-E server side. Even if Expressway-C is able to connect to this address, it is not correct as the SIP SERVICE message is intended for Expressway-C to receive and process.

SIP SERVICE message arrives to Expressway-C:

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,973" Module="network.sip"
Level="DEBUG":  Action="Received"  Local-ip="10.0.30.2"  Local-port="27901"  Src-
ip="64.100.0.10"  Src-port="7003"  Msg-Hash="123456789123456789"
 SIPMSG:
 |SERVICE sip:serviceserver@cucm02.example.local SIP/2.0
 Via: SIP/2.0/TLS 64.100.0.10:7003;egress-zone=UCTraversal;branch=[branchID];proxy-call-
id=[callid];rport
 Via: SIP/2.0/TCP 127.0.0.1:5060;branch=[branchID];received=127.0.0.1;rport=25063;ingress-
zone=DefaultZone
 Call-ID: abcd12345678@127.0.0.1
 CSeq: 4616 SERVICE
 Contact: <sip:serviceproxy@cucm02.example.local>
 From: <sip:serviceproxy@cucm02.example.local>;tag=0987654321aaaa
 To: <sip:serviceserver@cucm02.example.local>
 Max-Forwards: 15
 Route: <sip:64.100.0.10:4401;transport=tls;apparent;ds;lr>
 Route: <sip:127.0.0.1:22210;transport=tcp;vcs-cate;lr>
 User-Agent: TANDBERG/4132 (X8.7.2)
 Date: Tue, 19 Apr 2016 07:09:13 GMT
 Event: service
 P-Asserted-Identity: <sip:serviceproxy@cucm02.example.local>
 X-TAATag: e90b4983919b1f7a46d38f835
 Identity:
"7ioJ9gpsS5ob2TUAttNxBGYRWDbnRuf5skrkxP+B14ngRvjkIWIu7BQP5W7vW1BTVyVaGuubV5u7rPDc5anDx9u46i/8Tkx
xYuxkr83DEh/cYPWlwO7JvTP5nub6/EtEt6RXvwizY6Gm/MXV4eMqQJ06kA86EFxP1SsRxop0YjUs61B10JnBrtQjOicskoA
uMGzNjiBKvcCAbrASGtWP015vRp9khcs3e8vmkpZH5Qtef6+gNaRWPES3MS=="
 Content-Type: multipart/mixed;boundary=boundary-6j7zrmj35ifsu3efg5ga603hnz1nbf
 Content-Length: 2555

 --boundary-6j7zrmj35ifsu3efg5ga603hnz1nbf
 Content-Type: application/text

 <?xml version="1.0" encoding="utf-8"?>
<methodCall><params><username>john.smith</username><realm>expe.example.com</realm><nonce>2i78wor
v9unccs6vbclfi4xai78worv9unccs6vbclfi4xa4i15j</nonce><qop>auth</qop><cnonce>54f80570</cnonce><nc
>00000001</nc><response>2i78worv9unccs6vbclfi4xa4i15j</response><uri>sip:cucm02.example.local</u
ri><method>REGISTER</method><id>12345678</id><caching-enabled>true</caching-
enabled><reqtype>collab-
edge</reqtype></params><methodName>DigestAuth</methodName><version>1.0</version><msgid>123456789
79</msgid><sipdomain>cucm02.example.local</sipdomain></methodCall>

 --boundary-6j7zrmj35ifsu3efg5ga603hnz1nbf
 Content-Type: application/x-x509-ca-cert
-----BEGIN CERTIFICATE-----
hknS5nQ8NJEspxLPY0N4BvA8iL7ZasOqnqgHRlj95N8bn
OfigoKhe90kV6Y7PRbRpwFv6jGiFR8hyepr3t2BPec0aZ
ZAK3ZC92RQbDjCxy2U99L8WLlTpJQwIuTjLHicbiNCNZu
```

```
Be9xEMgewwGFVfSzW08DzlecJNXpsKqQ0ivbpLbwreXJG
SCbcse3O67yvghMDsotcK4gur11FZWOZJFa3EMlgoT3Mj
ApGvMfL9caTjY1EaLWDl5rWGGe8FpRLCizrz0wwUGg7Px
Moy6kAujtolwN9BUI0sgJ98MnBuuREJZNW7g7nJL5zywT
FXhMgy9PBUMuwjgu5KruY4caWDYtNu1kZzCtnm044lOk7
xhIOoOWWj9sNFnDQGDrgBIFBjggEihSbZr6h4Pq2ZMZ4r
i5yGpz0j7a6lg2NOKm6FXpfqVlB7zvyQsM6x0XJEImpjV
al0nHYkTLkBEmK5jVosgyOrSWpZPimc364sRxRW4ABZZX
M6XstZNGhvQNDVk1JlfCN5yRtEgEkkizeWOHJcts922wL
2rVTfUfWGXMkca8YHKj2ixkthNnHVbLG0YoUNOUDHq1xu
49F7Kcw7neuQQZ4MmEif59lnyhY7qEIQVEpGn0jgqZAX8
omNVxTewa9nTXvjxo5xvTLghYfESCqniBbtWwMhhRuR7N
eh09OvFWsuUyHJmDBYpoNZWTXEB4Fw5XwfjzZAoHzOFV6
xcE4LGYrpI4EbaZ58r8uVrfXkrNrgepFw2zMgamhwf9n5
AzEU2gh9vTUNZEAn8De5XQKAipeehO8Dpef2JTBLV5avf
nh7rfxh8BZY4xteSRox8iBnT4Na6qsDMb2gvp6gTYFFJH
RGMHIe5siI1HhARqDjen4EwrKfMOYNJWTqmx4mjDrqyme
 -----END CERTIFICATE-----
```

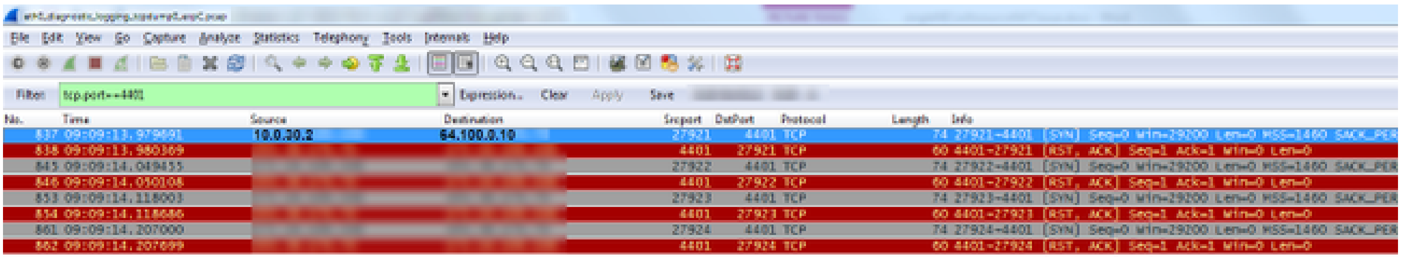
|

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,977"
Module="developer.sip.leg" Level="INFO"
CodeLocation="ppcmains/sip/sipproxy/SipProxyLeg.cpp(10047)"
Method="SipProxyLeg::routeViaNettleIfNeeded" Thread="0x3150905deea6":  this="0xc76759f343ca"
Type="Outbound"  routingViaNettle="false"  twoInARow="false" oneIsATraversalServerZone="false"
isCall="false" isRefer="false" fromClusterPeer="false" fromNettle="false" toNettle="false"
inboundZone=UC_Traversal (encryption-mode=on ice-mode=off) outboundZone=DefaultZone (encryption-
mode=auto ice-mode=off) encryptionSettingsRequireNettle="true" iceSettingsRequireNettle="false"
needlesslyNettling="false" routeViaNettle="false"
```

Expressway-C tries to send this SIP SERVICE message as to what it shows in the Route header, but connection fails:

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,979" Module="network.tcp"
Level="DEBUG":  Src-ip="10.0.30.2" Src-port="27921" Dst-ip="64.100.0.10" Dst-port="4401"
Detail="TCP Connecting"
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,980" Module="network.tcp"
Level="ERROR":  Src-ip="10.0.30.2" Src-port="27921" Dst-ip="64.100.0.10" Dst-port="4401"
Detail="TCP Connection Failed"
```

In the packet capture of Expressway-C the TCP SYN attempt gets a RST response:



Filter: tcp.port==4401

No.	Time	Source	Destination	Srcport	DstPort	Protocol	Length	Info
837	09:09:13.979691	10.0.30.2	64.100.0.10	27921	4401	TCP	74	27921→4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
838	09:09:13.980369	[redacted]	[redacted]	4401	27921	TCP	60	4401→27921 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
845	09:09:14.049455	[redacted]	[redacted]	27922	4401	TCP	74	27922→4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
846	09:09:14.050108	[redacted]	[redacted]	4401	27922	TCP	60	4401→27922 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
853	09:09:14.118003	[redacted]	[redacted]	27923	4401	TCP	74	27923→4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
854	09:09:14.118686	[redacted]	[redacted]	4401	27923	TCP	60	4401→27923 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
861	09:09:14.207000	[redacted]	[redacted]	27924	4401	TCP	74	27924→4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
862	09:09:14.207699	[redacted]	[redacted]	4401	27924	TCP	60	4401→27924 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The result is that Expressway-C sends a 408 Request Timeout towards the Expressway-E:

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,982" Module="network.sip"
Level="INFO":  Action="Sent"  Local-ip="10.0.30.2"  Local-port="27901"  Dst-ip="64.100.0.10"
Dst-port="7003"   Detail="Sending Response Code=408, Method=SERVICE, CSeq=4616,
To=sip:serviceserver@cucm02.example.local, Call-ID=abcd12345678@127.0.0.1, From-
Tag=0987654321aaaa, To-Tag=0987654321bbbb, Msg-Hash=123456789123456789"
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,982" Module="network.sip"
Level="DEBUG":  Action="Sent"  Local-ip="10.0.30.2"  Local-port="27901"  Dst-ip="64.100.0.10"
Dst-port="7003"  Msg-Hash="123456789123456789"
```

```
 SIPMSG:
 |SIP/2.0 408 Request Timeout
 Via: SIP/2.0/TLS 64.100.0.10:7003;egress-zone=UCTraversal;branch=[branchID];proxy-call-id=[callid];received=64.100.0.10;rport=7003;ingress-zone=UCTraversal;ingress-zone-id=4
 Via: SIP/2.0/TCP 127.0.0.1:5060;branch=[branchID];received=127.0.0.1;rport=25063;ingress-zone=DefaultZone
 Call-ID: abcd12345678@127.0.0.1
 CSeq: 4616 SERVICE
 From: <sip:serviceproxy@cucm02.example.local>;tag=0987654321aaaa
 To: <sip:serviceserver@cucm02.example.local>;tag=0987654321bbbb
 Server: TANDBERG/4132 (X8.7.2)
 Warning: 399 10.0.30.2:5061 "Request Timeout"
 Content-Length: 0
```

Solution

There are two possible solutions to this condition.

Disable the source IP port translation on the firewall

If you disable the source IP/port translation on the firewall, Expressway-E server views Expressway-C traffic as arriving from 10.0.30.2:27901 (actual IP and port on the Expressway-C) instead of 64.100.0.10:4401 (NAT address). In this way, the Route header on the SIP SERVICE message contains 10.0.30.2:27901 value and on receipt of this message, the Expressway-C will route it to itself and do some processing on it resulting in a 200 OK to be sent back to the Expressway-E (if all goes fine) which will then proxy through the SIP REGISTER message to continue the registration process.

Move to a dual NIC configuration

With a dual NIC configuration on Expressway-E, NAT reflection need not be performed and the issue is avoided. However, ensure that the internal firewall between Expressway-E and Expressway-C (if present) is not doing source IP/port translation from traffic from Expressway-C to Expressway-E (which would result in similar issues).

Related Information

- Supported network deployments for Expressway are detailed in Appendix 4 of the Expressway Basic Configuration Guide
- Follow the ASA configuration details in order to configure supported Expressway network deployments