

# NAT リフレクション上の送信元 IP アドレス変換による MRA 電話サービスの失敗 ( スタティック NAT 有効時の単一 NIC 設定 )

## 目次

[概要](#)

[前提条件](#)

[使用するコンポーネント](#)

[背景説明](#)

[問題](#)

[ネットワーク図](#)

[詳細](#)

[診断 ログの証拠](#)

[解決策](#)

[ファイアウォールのソース IP ポート変換を無効にしてください](#)

[二重 NIC 設定に移動してください](#)

[関連情報](#)

## 概要

この資料にスタティック NAT 設定の Expressway-E 単一 NIC で NAT リフレクション上のソース IP 変換によって引き起こされる MRA 上の電話サービス失敗を解決する方法を記述されています。

## 前提条件

次の項目に関する知識が推奨されます。

- Network Address Translation ( NAT; ネットワーク アドレス変換 )
- SIP ( Session Initiation Protocol )
- Cisco ビデオ コミュニケーション サーバ ( VCS ) または Expressway 基本設定
- Expressway または VCS 上の Mobile and Remote Access ( MRA )

## 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

注: 全体の資料によって、Expressway デバイスは Expressway-E および Expressway C と呼ばれます。ただし、同じ設定はビデオ コミュニケーション コミュニケーション・サーバ (VCS) Expressway および VCS 制御装置に適用されます。

## 背景説明

この資料は Mobile and Remote Access が単一 NIC およびスタティック NAT アドレスを使用して Expressway-E の Expressway で展開された scenario を取り扱っています ( Expressway 基本設定ガイドに記述されているように Expressway-E 単一 LAN インターフェイスを使用して 3 ポート ファイアウォール DMZ として、記述されている )。MRA ユーザはログインに正常にできましたが、しかし電話サービスにアクセスできません。

外部クライアントからの SIP レジスタ メッセージはポート 5061 で Expressway-E によって受け取りに成功します。

Expressway-E はそれから Expressway C の方の SIP サービス メッセージを作成します。この要求は 408 要求タイムアウトという結果に終わります。

## 問題

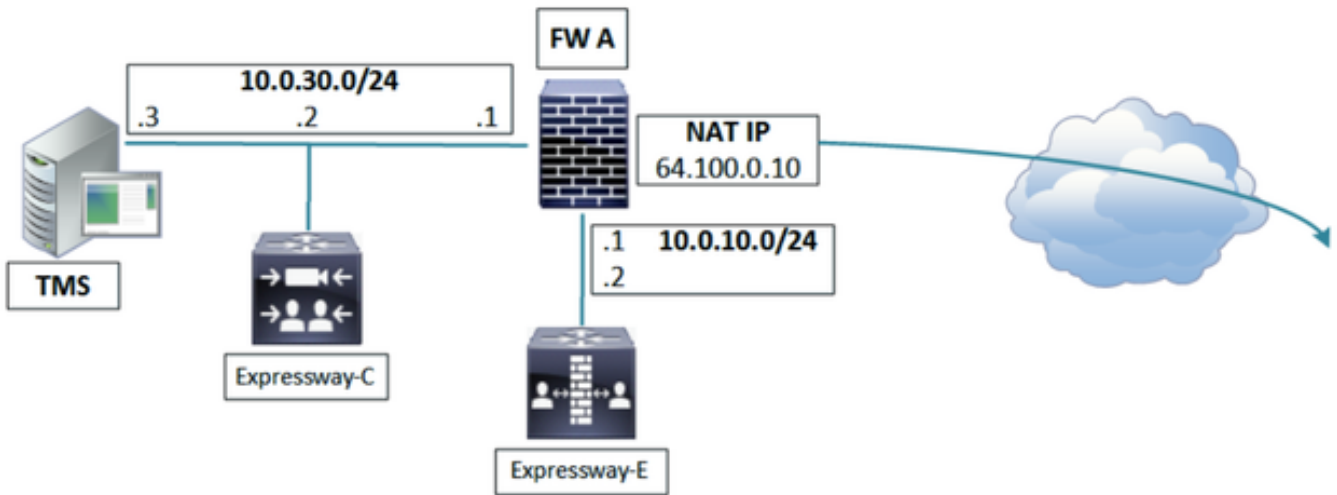
電話サービスは SIP レジスタ メッセージが Cisco Unified Communications Manager に行かないので失敗します ( CUCM が Call Manager )。Expressway-E および Expressway C は SIP サービス メッセージ交換を使用して証明書をきちんと交換できません。SIP サービス メッセージは Expressway C から応答としてだけ 408 要求タイムアウトを得ます。SIP サービス メッセージが正常ではないので、Expressway-E は Expressway C に SIP レジスタ メッセージを転送しません

これは Expressway C と Expressway-E 間のファイアウォールが Expressway C から Expressway-E にメッセージのための IP ( およびポート ) 変換のソースをたどるという事実によって引き起こされます。これは自身のローカルアドレスの代わりにその変換アドレスの方にそれらの SIP サービス メッセージを、不正確にルーティングする Expressway C という結果に終わります。正常なシナリオでは、Expressway C は SIP サービス メッセージ自体を処理します。

( Expressway-E と Expressway C 間の SIP サービス メッセージが証明書をチェックするのに使用され、従って traversal zone 設定の始めに、または MRA 上の最初登録にしか見られません。 )

## ネットワーク図

次のイメージはこの資料の全体にわたって参照ように使用されるネットワークダイアグラムの例を提供します、:



## 詳細

Expressway C パケットキャプチャから、ことが Expressway C わかります ( 10.0.30.2 )  
 Expressway-E スタティック NAT パブリックIPアドレスへの接続に成功します ( 64.100.0.10 ) ポート 7003 で。 ( 送信元ポートが Expressway C の 27901 であるという ) 表記:

No.	Time	Source	Destination	Support	DestPort	Protocol	Length	Info
80	09:09:04.879232	10.0.30.2	64.100.0.10	27901	7003	TCP	1034	27901->7003 [PSH, ACK] Seq=1 Ack=909 win=1392 Len=395 TSval=149210902 TSecr=149210902
81	09:09:04.882228			7003	27901	TCP	66	27901->7003 [ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=149210902 TSecr=149210902
82	09:09:04.882270			27901	7003	TCP	66	27901->7003 [ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=149210902 TSecr=149210902
83	09:09:04.884037			27901	7003	TCP	1419	27901->7003 [PSH, ACK] Seq=909 Ack=596 win=1384 Len=1353 TSval=149210902 TSecr=149210902
84	09:09:04.894490			7003	27901	TCP	1078	7003->27901 [PSH, ACK] Seq=596 Ack=2322 win=1392 Len=1032 TSval=149210905 TSecr=149210905
85	09:09:04.933990			27901	7003	TCP	66	27901->7003 [ACK] Seq=2322 Ack=1608 win=1384 Len=0 TSval=149210915 TSecr=149210915
831	09:09:13.972925			7003	27901	TCP	1514	7003->27901 [ACK] Seq=1608 Ack=2322 win=1392 Len=1448 TSval=149219992 TSecr=149210902
832	09:09:13.973976			27901	7003	TCP	66	27901->7003 [ACK] Seq=2322 Ack=3056 win=1384 Len=0 TSval=149219992 TSecr=149219992
833	09:09:13.972343			7003	27901	TCP	1514	7003->27901 [ACK] Seq=3056 Ack=2322 win=1392 Len=1448 TSval=149219992 TSecr=149210902
834	09:09:13.972365			27901	7003	TCP	66	27901->7003 [ACK] Seq=2322 Ack=4504 win=1384 Len=0 TSval=149219992 TSecr=149219992

Expressway-E のパケットキャプチャで接続が ( 自身のスタティック NAT パブリックIPアドレスである ) 宛先 10.0.10.2 が付いているポート 4401 およびポート 7003 の 64.100.0.10 から来るということがわかります:

No.	Time	Source	Destination	Support	DestPort	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=1392 Len=395 TSval=149210902 TSecr=149210902
34	09:09:04.882482			7003	4401	TCP	66	7003->4401 [PSH, ACK] Seq=1 Ack=909 win=1392 Len=395 TSval=149210902 TSecr=149210902
35	09:09:04.883342			4401	7003	TCP	66	4401->7003 [ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=149210902 TSecr=149210902
36	09:09:04.883368			4401	7003	TCP	1419	4401->7003 [PSH, ACK] Seq=909 Ack=596 win=1384 Len=1353 TSval=149210902 TSecr=149210902
37	09:09:04.894747			7003	4401	TCP	1078	7003->4401 [PSH, ACK] Seq=596 Ack=2322 win=1392 Len=1032 TSval=149210905 TSecr=149210905
38	09:09:04.933008			4401	7003	TCP	66	4401->7003 [ACK] Seq=2322 Ack=1608 win=1384 Len=0 TSval=149210915 TSecr=149210915
923	09:09:13.972986			7003	4401	TCP	2962	7003->4401 [ACK] Seq=1608 Ack=2322 win=1392 Len=2896 TSval=149219992 TSecr=149210902
924	09:09:13.972018			7003	4401	TCP	1206	7003->4401 [PSH, ACK] Seq=4504 Ack=2322 win=1392 Len=1140 TSval=149219992 TSecr=149210902

これらは Expressway C および E 間の接続の観点です:

Expressway C: 10.0.30.2:27901 <-> 64.100.0.10:7003

Expressway-E: 64.100.0.10:4401 <-> 10.0.10.2:7003

これは Expressway C と Expressway-E 間のファイアウォールがそれらのメッセージのソース IP およびポート変換をしていることを示します。

Expressway-E の SIP コミュニケーションのフローを一覧する場合、Expressway C によって証明書を交換するために Expressway-E が SIP サービス メッセージを生成するがこれが 408 の要求タイムアウトという結果に終ることを見る事ができます MRA クライアントデバイスから SIP レジスタを得ることを。

## 診断 ログの証拠

この SIP サービス メッセージのルート ヘッダが ( Expressway-E から Expressway C に送信される ) NAT アドレス ( 64.100.0.10:4401 ) の IP およびポートが含まれていることに注意して下さい。

このメッセージが Expressway C で着くとき、Expressway C は 64.100.0.10:4401 の方のそのルート ヘッダに、基づいてメッセージをルーティングを試みます。これはこのアドレスが Expressway-E サーバ側にあるのでそれがこのアドレスへの接続をされないので失敗します。Expressway C はこのアドレスに接続できても Expressway C が受け取り、処理することができないように SIP サービス メッセージが意図されているので正しくありません。

SIP サービス メッセージは Expressway C に着きます:

```
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/cYPWlw07JvTP5nub6/EtEt6RXvwizY6Gm/MXV4eMqQJ06kA86EFxP1SsRxop0YjUs61B10JnBrtQjOicskoA
uMGzNjBKvcCAbrASgtWP015vRp9khcs3e8vmkpZH5QtEf6+gNaRWPES3MS=="
Content-Type: multipart/mixed;boundary=boundary-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Length: 2555

--boundary-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Type: application/text

<?xml version="1.0" encoding="utf-8"?>
<methodCall><params><username>john.smith</username><realm>expe.example.com</realm><nonce>2i78wor
v9unccs6vbc1fi4xai78worv9unccs6vbc1fi4xa4i15jk</nonce><qop>auth</qop><cnonce>54f80570</cnonce><nc
>00000001</nc><response>2i78worv9unccs6vbc1fi4xa4i15jk</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-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Type: application/x-x509-ca-cert
-----BEGIN CERTIFICATE-----
hknS5nQ8NJEspXLPY0N4BvA8iL7ZasOqngqHRlj95N8bn
```

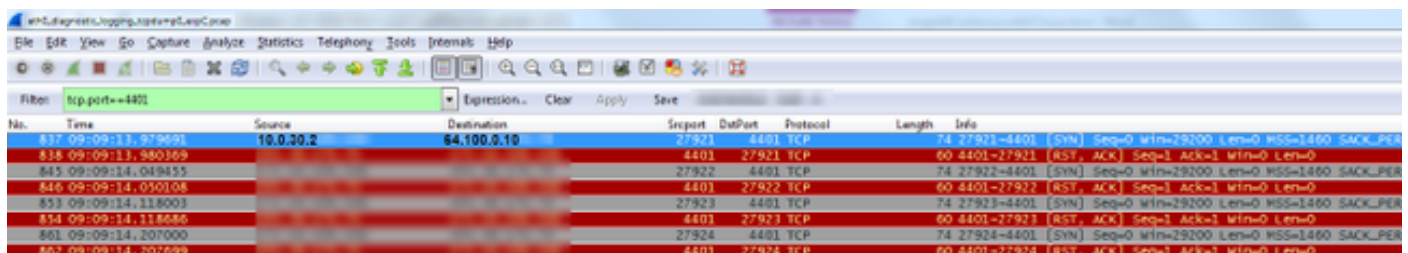
```
OfigoKhe90kV6Y7PRbRpwFv6jGiFR8hyepr3t2BPec0aZ
ZAK3ZC92RQbdjCxy2U99L8WLLTpJQwIuTjLHicbiNCNZu
Be9xEMgewwGFVfSzW08DzlecJNXpsKqQ0ivbplbwreXJG
SCbcse3067yvghMDsotcK4gur11fZWOZJFa3EMlgoT3Mj
ApGvMfL9caTjY1EaLWD15rWGGe8FpRLCizrZ0wwUGg7Px
Moy6kAu jtolwN9BUI0sgJ98MnBuuREJZNW7g7nJL5zyWT
FXhMgy9PBUMuwjgu5KruY4caWDYtNu1kZzCtnm0441Ok7
xhIOoOWWj9sNFndQGDrgBIFBjggEihSbZr6h4Pq2ZMZ4r
i5yGpz0j7a6lg2NOKm6FXpfqV1B7zvyQsM6x0XJEImpjV
al0nHYkTLkBEk5jVosgyOrSWpZPimc364sRxRW4ABZZX
M6XstZNGhvQNDVklJlfcN5yRtEgEkkizeWOHJcts922wL
2rVTfUfWGXmkca8YHKj2ixkthNnHVbLG0YoUNOUdHq1xu
49F7Kcw7neuQQZ4MmEif59lnyhY7qEIQVEpGn0jggZAX8
omNVxTewa9nTXvjxo5xvTLghYfESCqniBbtWwMhhRuR7N
eh09OvFwsuUyHJmDBYpoNZWTXEB4Fw5XwfjzZaOHzOFV6
xcE4LGYrpI4EbaZ58r8uVrfXkrNrgepFw2zmgamhfw9n5
AzEU2gh9vTUNZEAn8De5XQKAipeeh08Dpef2JTBLV5avf
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/siproxy/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 は送信 することをルート ヘッダで示すが、接続は失敗しますものに関してこの SIP サービス メッセージを試みます:

```
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"
```

Expressway C のパケットキャプチャで TCP SYN 試みは RST 応答があります:



No.	Time	Source	Destination	SrcPort	DstPort	Protocol	Length	Info
817	09:09:13.979691	10.0.30.2	64.100.0.10	27921	4401	TCP	74	27921->4401 [SYN] Seq=0 Win=28200 Len=0 MSS=3460 SACK_PER
818	09:09:13.980369			4401	27921	TCP	60	4401->27921 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
845	09:09:14.049451			27922	4401	TCP	74	27922->4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
846	09:09:14.050108			4401	27922	TCP	60	4401->27922 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
853	09:09:14.118001			27923	4401	TCP	74	27923->4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
854	09:09:14.118586			4401	27923	TCP	60	4401->27923 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
861	09:09:14.207000			27924	4401	TCP	74	27924->4401 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
862	09:09:14.207699			4401	27924	TCP	60	4401->27924 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

結果は Expressway C が Expressway-E の方の 408 要求タイムアウトを送信 することです:

```
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@cucom2.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
```

## 解決策

この状態へ 2 つの可能な解決策があります。

### ファイアウォールのソース IP ポート変換を無効にしてください

ファイアウォールのソース IP/port 変換を無効にする場合、Expressway-E サーバは見ま ( Expressway C の実際の IP およびポート ) 64.100.0.10:4401 の代りに 10.0.30.2:27901 から着きますように Expressway C トラフィックを ( NAT アドレス )。このように、SIP サービスメッセージのルートヘッダは 10.0.30.2:27901 値を示し、このメッセージの受信で、( SIP レジスタメッセージを通したプロキシ登録 手続きを続けるすべてがうまく行けば ) Expressway C はそれ自身にそれをルーティングし、Expressway-E に送返されるべき 200 OK に終わってそれで処理する一部をします。

### 二重 NIC 設定に移動してください

Expressway-E の二重 NIC 設定によって、NAT リフレクションは実行された必要はないし、問題は避けます。ただし Expressway-E と Expressway C 間の内部ファイアウォールが ( もしあれば ) Expressway C からの ( 同じような問題という結果に終る ) にトラフィックからソース IP/port 変換を Expressway-E していないことを、確認してください。

## 関連情報

- Expressway のためのサポートされたネットワーク配置は [Expressway 基本設定ガイド](#) の付録 4 で詳述されます
- サポートされた Expressway ネットワーク配置を設定するために [ASA コンフィギュレーションの詳細](#) に続いて下さい