

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)

内容

[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](#)

[解決方法](#)

[ファイアウォールの送信元IPポート変換を無効にする](#)

[デュアルNIC構成に移行する](#)

[関連情報](#)

概要

このドキュメントでは、スタティックNAT設定のExpressway-EシングルNICを使用した、NATリフレクションを介した送信元IP変換が原因で発生するMRAでの電話サービス障害のトラブルシューティング方法について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Network Address Translation (NAT; ネットワーク アドレス変換)
- SIP (Session Initiation Protocol)
- Cisco Video Communication Server(VCS)またはExpresswayの基本設定
- ExpresswayまたはVCS経由のモバイルおよびリモートアクセス(MRA)

使用するコンポーネント

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

注:文書全体を通じて、ExpresswayデバイスはExpressway-EおよびExpressway-Cと呼ばれます。ただし、Video Communication Server(VCS)ExpresswayおよびVCS Controlデバイスにも同じ設定が適用されます。

背景説明

このドキュメントでは、モバイルおよびリモートアクセス(MRA)が、単一のNICとスタティック NATアドレスを使用してExpressway-EでExpresswayに導入されたシナリオについて説明します (『Expressway基本設定ガイド』を参照)。MRAユーザは正常にログインできますが、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 REGISTERメッセージがExpressway-Eによってポート5061で正常に受信されます。

次に、Expressway-EがExpressway-CへのSIP SERVICEメッセージを作成します。この要求により、408 Request Timeoutが発生します。

問題

SIP REGISTERメッセージがCisco Unified Communications Manager (CUCMまたはCall Manager) に送信されないため、電話サービスが失敗します。 Expressway-EとExpressway-Cは、SIP SERVICEメッセージ交換を使用して証明書を正しく交換できません。SIP SERVICEメッセージは、Expressway-Cからの応答として408 Request Timeoutのみを取得します。SIP SERVICEメッセージが成功しないため、Expressway-EはSIP REGISTERメッセージをExpressway-Cに転送しません。

これは、Expressway-CとExpressway-Eの間のファイアウォールが、Expressway-CからExpressway-Eへのメッセージの送信元IP (およびポート) 変換を行っていることが原因です。その結果、Expressway-CはこれらのSIP SERVICEメッセージを、自身のローカルアドレスではなく、変換されたアドレスに誤ってルーティングします。成功したシナリオでは、Expressway-CがSIP SERVICEメッセージ自体を処理します。(Expressway-EとExpressway-Cの間のSIP SERVICEメッセージは、証明書のチェックに使用されるため、トラバーサルゾーンの設定の開始時またはMRAでの最初の登録時にのみ表示されます)。

ネットワーク図

次の図は、このドキュメント全体の参照として使用されるネットワークダイアグラムの例を示しています。

診断ログの証拠

このSIP SERVICEメッセージ (Expressway-EからExpressway-Cに送信) のルートヘッダーには、NATアドレス(64.100.0.10:4401)のIPとポートが含まれていることに注意してください。このメッセージがExpressway-Cに到着すると、Expressway-Cはそのルートヘッダーに基づいて、64.100.0.10:4401に向けてメッセージのルーティングを試みます。このアドレスはExpressway-Eサーバ側にあるため、このアドレスに接続できないため、失敗します。Expressway-Cがこのアドレスに接続できる場合でも、SIP SERVICEメッセージはExpressway-Cが受信して処理することを目的としているため、正しくありません。

SIP SERVICEメッセージがExpressway-Cに到達します。

```
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:
"7ioJ9gpsS5ob2TUAttNxBGYRWDbnRuf5skrxxP+B14ngRvjkIWIu7BQP5W7vW1BTVyVaGuubV5u7rPDc5anDx9u46i/8Txx
xYuxkr83DEh/cYPWlw07JvTP5nub6/EtEt6RXvwizY6Gm/MXV4eMqQJ06kA86EFxP1SsRxop0YjUs6lB10JnBrtQjOicskoA
uMGzNjiBKvcCAbrASgtWP015vRp9khcs3e8vmkpZH5Qtef6+gNaRWPEs3MS=="
Content-Type: multipart/mixed;boundary=boundary-6j7zrmj35ifsu3efg5ga603hznzlnbf
Content-Length: 2555

--boundary-6j7zrmj35ifsu3efg5ga603hznzlnbf
Content-Type: application/text

<?xml version="1.0" encoding="utf-8"?>
<methodCall><params><username>john.smith</username><realm>expe.example.com</realm><nonce>2i78wor
v9unccs6vbclfi4xa178worv9unccs6vbclfi4xa4i15j</nonce><qop>auth</qop><nonce>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-6j7zrmj35ifsu3efg5ga603hznzlnbf
Content-Type: application/x-x509-ca-cert
-----BEGIN CERTIFICATE-----
hknS5nQ8NJEspxLPY0N4BvA8iL7ZasOqnqgHRlj95N8bn
OfigoKhe90kV6Y7PRbRpwFv6jGiFR8hyepr3t2BPec0aZ
```

```
ZAK3ZC92RQbdJcXy2U99L8WLLTpJQwIuTjLHicbiNCNZu
Be9xEMgewwGFVfSzW08DzlecJNXpsKqQ0ivbplbwreXJG
SCbcse3067yvghMDsotcK4gur11FZWOZJFa3EMlgoT3Mj
ApGvMfL9caTjY1EaLWD15rWGGe8FpRLCizrZ0wwUGg7Px
Moy6kAujtolwN9BUI0sgJ98MnBuuREJZNW7g7nJL5zyWT
FXhMgy9PBUmuwjgu5KruY4caWDYtNu1kZzCtnm0441Ok7
xhIOoOWWj9sNFndQGDrgBIFBjggEihSbZr6h4Pq2ZMZ4r
i5yGpz0j7a6lg2NOKm6FXpfqV1B7zvyQsM6x0XJEImpjV
al0nHYkTLkBEk5jVosgyOrSWpZPimc364sRxRW4ABZXX
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/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は、ルートヘッダーに表示される内容に関してこのSIP SERVICEメッセージを送信しようとはしますが、接続は失敗します。

```
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の試行がRST応答を受信します。

No.	Time	Source	Destination	Sport	DstPort	Protocol	Length	Info
817	09:09:13.979091	10.0.30.2	64.100.0.10	27921	4401	TCP	74	27921->4401 [SYN] Seq=0 Win=28200 Len=0 MSS=3460 SACK_PERM=1
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=28200 Len=0 MSS=3460 SACK_PERM=1
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=28200 Len=0 MSS=3460 SACK_PERM=1
854	09:09:14.118086			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=28200 Len=0 MSS=3460 SACK_PERM=1
862	09:09:14.207099			4401	27924	TCP	60	4401->27924 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

その結果、Expressway-CがExpressway-Eに対して408要求タイムアウトを送信します。

```
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
```

解決方法

この状況に対する2つの解決策があります。

ファイアウォールの送信元IPポート変換を無効にする

ファイアウォールで送信元IP/ポート変換を無効にすると、Expressway-Eサーバは、10.0.30.2:27901 (Expressway-Cの実際のIPおよびポート) から64.100.0.10:4401 (NATアドレス) ではなくExpressway-Cトラフィックをと見します。これにより、SIP SERVICEメッセージのルートヘッダーに10.0.30.2:27901の値が含まれ、このメッセージを受信すると、Expressway-Cは自身にルーティングし、処理を行って、200 OKをExpressway-Eに送り返します (すべて問題問題の問題のある場合) プロセス。

デュアルNIC構成に移行する

Expressway-EのデュアルNIC設定では、NATリフレクションを実行する必要はなく、問題は回避されます。ただし、Expressway-EとExpressway-Cの間の内部ファイアウォール (存在する場合) が、Expressway-CからExpressway-Eへのトラフィックからの送信元IP/ポート変換を行っていないことを確認します (同様の問題が発生します)。

関連情報

- Expresswayでサポートされるネットワークの展開については、『[Expressway Basic Configuration Guide](#)』の付録4を参照してください
- サポートされている[Expresswayネットワーク展開](#)を設定するには、ASAの設定の詳細に従います