

MRA-Telefondienste fehlschlagen aufgrund der Quell-IP-Übersetzung über NAT-Reflektion (einzelne NIC-Konfiguration mit aktivierter statischer NAT)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Netzwerkdiagramm](#)

[Details](#)

[Beweise für Diagnoseprotokolle](#)

[Lösung](#)

[Deaktivieren Sie die Quell-IP-Port-Übersetzung auf der Firewall.](#)

[Wechsel zu einer Konfiguration mit zwei NICs](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie bei einem Ausfall der Telefondienste über MRA, der durch die IP-Quellübersetzung über NAT-Reflektion verursacht wird, mit einer Expressway-E Single-NIC mit statischer NAT-Konfiguration Fehler beheben können.

Voraussetzungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- NAT (Network Address Translation)
- SIP (Session Initiation Protocol)
- Grundkonfiguration des Cisco Video Communication Server (VCS) oder Expressway
- Mobiler und Remote-Zugriff (MRA) über Expressway oder VCS

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: Expressway-Geräte werden im gesamten Dokument als Expressway-E und Expressway-C bezeichnet. Die gleiche Konfiguration gilt jedoch auch für Video Communication Server (VCS) Expressway- und VCS Control-Geräte.

Hintergrundinformationen

Dieses Dokument behandelt ein Szenario, in dem Mobil- und Remote-Zugriff auf Expressway mit Expressway-E mithilfe einer einzigen NIC und einer statischen NAT-Adresse bereitgestellt wurde (beschrieben als 3-Port-Firewall DMZ mit Single Expressway-E LAN Interface, wie im Expressway Basic Configuration Guide beschrieben). MRA-Benutzer können sich erfolgreich anmelden, haben jedoch keinen Zugriff auf Telefondienste.

Die SIP-REGISTER-Nachricht von einem externen Client wird von Expressway-E erfolgreich an Port 5061 empfangen.

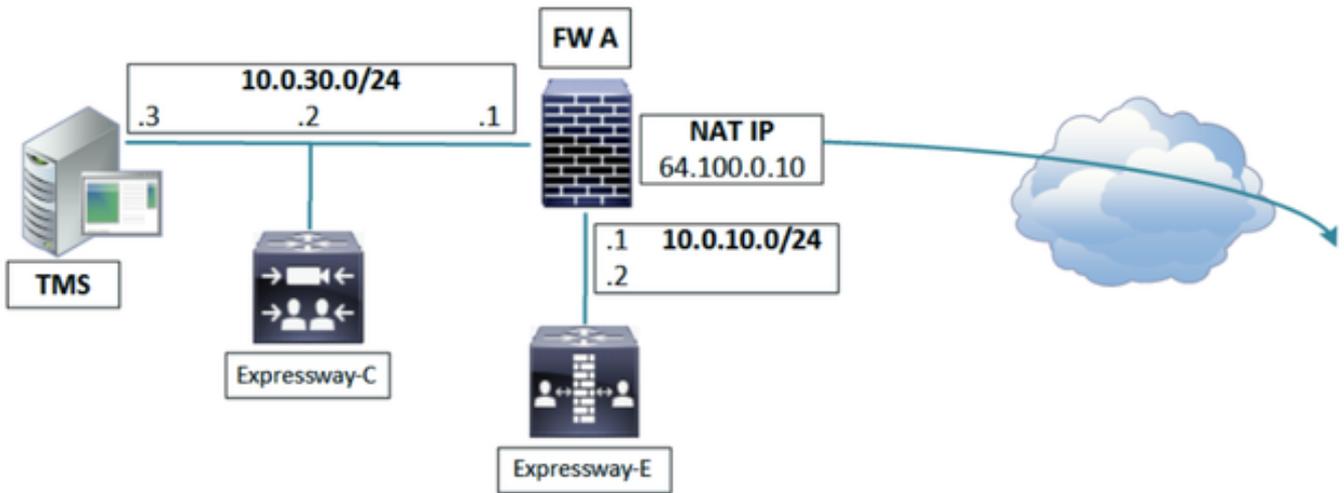
Expressway-E erstellt dann eine SIP-SERVICE-Nachricht an Expressway-C. Diese Anfrage resultiert in einem 408 Request Timeout.

Problem

Telefondienste schlagen fehl, da die SIP-REGISTER-Nachricht nicht an den Cisco Unified Communications Manager (CUCM oder Call Manager) weitergeleitet wird. Expressway-E und Expressway-C sind nicht in der Lage, ihre Zertifikate ordnungsgemäß über den SIP SERVICE Message Exchange auszutauschen. Die SIP-SERVICE-Nachrichten erhalten nur ein 408 Request Timeout als Antwort vom Expressway-C. Da die SIP-SERVICE-Nachricht nicht erfolgreich ist, leitet das Expressway-E die SIP-REGISTER-Nachricht nicht an den Expressway-C weiter. Dies liegt daran, dass die Firewall zwischen Expressway-C und Expressway-E die Quell-IP (und Port)-Übersetzung für Nachrichten vom Expressway-C zum Expressway-E durchführt. Dies führt dazu, dass Expressway-C diese SIP-SERVICE-Nachrichten fälschlicherweise an die übersetzte Adresse anstatt an die eigene lokale Adresse weiterleitet. In einem erfolgreichen Szenario verarbeitet Expressway-C die SIP-SERVICE-Nachricht selbst. (Die SIP-SERVICE-Nachricht zwischen Expressway-E und Expressway-C wird zur Prüfung von Zertifikaten verwendet und wird daher nur zu Beginn einer Traversal Zone-Einrichtung oder bei der ersten Registrierung über MRA angezeigt.)

Netzwerkdiagramm

Das folgende Bild zeigt ein Beispiel für ein Netzwerkdiagramm, das in diesem Dokument als Referenz verwendet wird:



Details

Aus den Expressway-C-Paketerfassungen können Sie sehen, dass der Expressway-C (10.0.30.2) erfolgreich mit der statischen öffentlichen IP-Adresse Expressway-E (64.100.0.10) an Port 7003 verbunden ist. (Beachten Sie, dass der Quellport auf dem Expressway-C "27901" lautet:

No.	Time	Source	Destination	SeqNum	Port	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=1492210902 TSecr=1492341627
81	09:09:04.882228			7003	27901	TCP	66	27901->7003 [ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=1492541630 TSecr=1492210902
82	09:09:04.882370			27901	7003	TCP	1419	27901->7003 [PSH, ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=1492541632 TSecr=1492210902
83	09:09:04.884037			7003	27901	TCP	1078	7003->27901 [PSH, ACK] Seq=596 Ack=2322 win=1392 Len=1032 TSval=1492210915 TSecr=1492541632
84	09:09:04.894490			27901	7003	TCP	66	27901->7003 [ACK] Seq=2322 Ack=1608 win=1384 Len=0 TSval=1492541682 TSecr=1492210915
85	09:09:04.933990			7003	27901	TCP	1514	7003->27901 [ACK] Seq=1608 Ack=2322 win=1392 Len=1448 TSval=1492219992 TSecr=1492541682
831	09:09:13.973915			27901	7003	TCP	66	27901->7003 [ACK] Seq=2322 Ack=3056 win=1384 Len=0 TSval=1492550720 TSecr=1492219992
832	09:09:13.973916			7003	27901	TCP	1514	7003->27901 [ACK] Seq=3056 Ack=2322 win=1392 Len=1448 TSval=1492219992 TSecr=1492541682
833	09:09:13.972343			27901	7003	TCP	66	27901->7003 [ACK] Seq=2322 Ack=4504 win=1384 Len=0 TSval=1492550720 TSecr=1492219992
834	09:09:13.972365			7003	27901	TCP	66	27901->7003 [ACK] Seq=2322 Ack=4504 win=1384 Len=0 TSval=1492550720 TSecr=1492219992

In der Paketerfassung des Expressway-E kann man sehen, dass die Verbindung von 64.100.0.10 auf Port 4401 (d. h. seine eigene statische öffentliche NAT-IP-Adresse) mit Ziel 10.0.10.2 und Port 7003 hergestellt wird:

No.	Time	Source	Destination	SeqNum	Port	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=1492541627 TSecr=1492190916
34	09:09:04.882482			7003	4401	TCP	66	7003->4401 [PSH, ACK] Seq=1 Ack=909 win=1392 Len=395 TSval=1492210902 TSecr=1492341627
35	09:09:04.883142			4401	7003	TCP	66	4401->7003 [ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=1492541630 TSecr=1492210902
36	09:09:04.883368			4401	7003	TCP	1419	4401->7003 [PSH, ACK] Seq=909 Ack=596 win=1384 Len=0 TSval=1492541632 TSecr=1492210902
37	09:09:04.894747			7003	4401	TCP	1078	7003->4401 [PSH, ACK] Seq=596 Ack=2322 win=1392 Len=1032 TSval=1492210915 TSecr=1492541632
38	09:09:04.933008			4401	7003	TCP	66	4401->7003 [ACK] Seq=2322 Ack=1608 win=1384 Len=0 TSval=1492541682 TSecr=1492210915
923	09:09:13.973986			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=1608 Ack=2322 win=1392 Len=1140 TSval=1492219992 TSecr=1492541682

Dies sind die Perspektiven der Verbindung zwischen Expressway-C und 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

Dies weist darauf hin, dass die Firewall zwischen Expressway-C und Expressway-E die Quell-IP- und Port-Übersetzung für diese Nachrichten durchführt.

Wenn Sie sich den SIP-Kommunikationsfluss auf Expressway-E anschauen, sehen Sie, dass der SIP-REGISTER vom MRA-Client-Gerät abgerufen wird. Anschließend generiert Expressway-E eine SIP-SERVICE-Nachricht, um seine Zertifikate mit dem Expressway-C auszutauschen. Dies führt jedoch zu einem 408 Request-Timeout.

Beweise für Diagnoseprotokolle

Beachten Sie, dass der Route-Header dieser SIP-SERVICE-Nachricht (von Expressway-E an Expressway-C gesendet) die IP-Adresse und den Port der NAT-Adresse (64.100.0.10:4401) enthält.

Wenn diese Nachricht auf dem Expressway-C eingeht, versucht Expressway-C, die Nachricht basierend auf diesem Route-Header an 64.100.0.10:4401 weiterzuleiten. Dies schlägt fehl, da es keine Verbindung zu dieser Adresse herstellen kann, da diese Adresse auf der Seite des Expressway-E Servers ist. Auch wenn Expressway-C eine Verbindung zu dieser Adresse herstellen kann, ist sie nicht korrekt, da die SIP-SERVICE-Nachricht für den Empfang und die Bearbeitung von Expressway-C vorgesehen ist.

Die SIP-SERVICE-Nachricht kommt bei Expressway-C an:

```
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:
"7ioJ9gpsS5ob2TUAttNxBGYRWDbnRuf5skrkrxP+B14ngRvjkiWIu7BQP5W7vW1BTvyVaGuubV5u7rPDc5anDx9u46i/8TxxYuxkr83DEh/cYPWlw07JvTP5nub6/EtEt6RXvwizY6Gm/MXV4eMqQJ06kA86EFxP1SsRxop0YjUs61B10JnBrTQjOicskoAuMGzNjIBKvcCAbrASGtWP015vRp9khcs3e8vmkpZH5Qtef6+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>2i78worv9unccs6vbclfi4xai78worv9unccs6vbclfi4xa4i15j</nonce><qop>auth</qop><cnonce>54f80570</cnonce><nc>00000001</nc><response>2i78worv9unccs6vbclfi4xa4i15j</response><uri>sip:cucm02.example.local</uri><method>REGISTER</method><id>12345678</id>< caching-enabled>true</caching-enabled><reqtype>collab-edge</reqtype></params><methodName>DigestAuth</methodName><version>1.0</version><msgid>12345678979</msgid><sipdomain>cucm02.example.local</sipdomain></methodCall>

--boundary-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Type: application/x-x509-ca-cert
-----BEGIN CERTIFICATE-----
```

hknS5nQ8NJEspXLpY0N4BvA8iL7ZasOqnqgHRl j95N8bn
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/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 versucht, diese SIP-SERVICE-Nachricht an die Angaben im Routen-Header zu
senden, die Verbindung schlägt jedoch fehl:

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"

Bei der Paketerfassung von Expressway-C erhält der TCP-SYN-Versuch eine RST-Antwort:

No.	Time	Source	Destination	SeqPort	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=1460 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=28200 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=28200 Len=0 MSS=1460 SACK_PER
854	09:09:14.118686			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=1460 SACK_PER
862	09:09:14.207699			4401	27924	TCP	60	4401->27924 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Das Ergebnis ist, dass Expressway-C ein 408 Request Timeout an Expressway-E sendet:

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
```

Lösung

Es gibt zwei mögliche Lösungen für diese Bedingung.

Deaktivieren Sie die Quell-IP-Port-Übersetzung auf der Firewall.

Wenn Sie die Quell-IP/Port-Übersetzung auf der Firewall deaktivieren, betrachtet der Expressway-E-Server den Expressway-C-Datenverkehr als von 10.0.30.2:27901 ankommend (tatsächliche IP und Port auf dem Expressway-C) anstatt von 64.100.0.10:4401 (NAT-Adresse). Auf diese Weise enthält der Routen-Header in der SIP-SERVICE-Nachricht den Wert 10.0.30.2:27901. Nach Erhalt dieser Nachricht leitet der Expressway-C die Nachricht an sich weiter und verarbeitet sie, sodass ein 200 OK an den Expressway-E zurückgesendet werden kann (wenn alles in Ordnung ist), der dann über die SIP REGISTER-Nachricht protrahiert Setzen Sie den Registrierungsprozess fort.

Wechsel zu einer Konfiguration mit zwei NICs

Bei einer Konfiguration mit zwei NICs auf Expressway-E muss keine NAT-Reflektion durchgeführt werden, und das Problem wird vermieden. Stellen Sie jedoch sicher, dass die interne Firewall zwischen Expressway-E und Expressway-C (sofern vorhanden) keine IP/Port-Quell-Übersetzung vom Datenverkehr von Expressway-C nach Expressway-E durchführt (was zu ähnlichen Problemen führen würde).

Zugehörige Informationen

- Unterstützte Netzwerkbereitstellungen für Expressway sind in Anhang 4 des [Expressway Basic Configuration Guide](#) detailliert beschrieben.
- Befolgen Sie die [ASA-Konfigurationsdetails](#), um die unterstützten Expressway-Netzwerkbereitstellungen zu konfigurieren.