Probleemoplossing voor de meeste gebruikelijke problemen voor zakelijke oproepen via snelweg

Inhoud

Inleiding

Dit document beschrijft de meest voorkomende problemen in de B2B-inzet (Business to Business). Hoe kan B2B problemen oplossen door snelwegen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Expressway-C (EXP-C)
- snelweg-E
- Cisco Unified Call Manager (CUCM)
- TelePresence Video Communication Server-C (VCS-C)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- snelweg C en E X8.1.1 of hoger
- Unified Communications Manager (CUCM) 10.0 of hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Gemeenschappelijke kwesties

1. Fout "//SIP/SIPTcp/wait_SdlReadRSP: Een groot bericht negeren. Laat slechts 5000 bytes toe. Verbinding terugstellen."

Bel TelePresence-endpoints die bij VCS zijn geregistreerd, vanaf een SIP-stam (Session Initiation Protocol) naar CUCM niet werken met "//SIP/SIPTcp/wait_SdlReadRSP: Een groot bericht negeren. Laat slechts 5000 bytes toe. Verbinding terugstellen."

De routingconfiguratie van de vraag in de snelweg-C/VCS-C is correct en de vraag wordt naar CUCM verzonden. SIP Invite bericht wordt verzonden naar CUCM, maar in de SDL logboeken zijn er geen SIP berichten. Deze fout is te zien in de SDL-bestanden:

"|AppInfo |SIPTcp - Een groot bericht van xxx.xxx.xxx:[27469] negeren. Laat slechts 5000 bytes toe. Verbinding terugstellen."

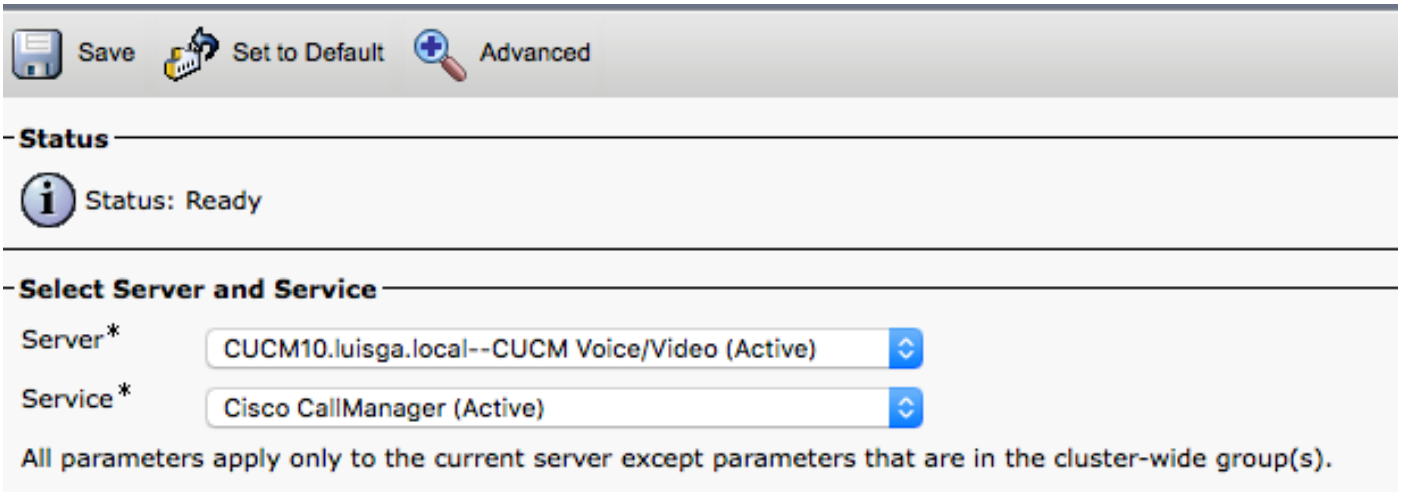
In CUCM 8.6 en onder de standaardwaarde voor SIP Max Inkomend Message Size was 5000, nadat CUCM 9.X is veranderd in 11000. Een upgrade van 8 of onder naar versie 9 of 10 zal echter de standaardwaarde in de vorige versie van de software behouden (5000).

Oplossing

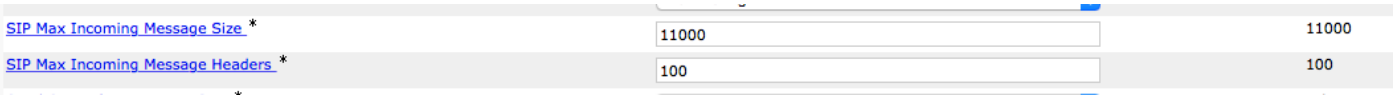
Dit probleem is gerelateerd aan bug CSCts00642

Vergroot de standaardwaarde van 5000 **MAX** aan een grootte die geschikt is voor dit soort oproepen voor de Geavanceerde Service Parameter **SIP**. 11000 lijkt een goede waarde te zijn voor het merendeel van de verwachte klantenscenario's.

Vanuit **CUCM Management Pagina,** navigeer **naar serviceparameters** en **selecteer** uw **CUCM-server en de CallManager Service**:



Selecteer de optie **Geavanceerd** en zoek naar **SIP Max Inkomend Berichtgrootte**:



2. Media streams stoppen als een andere gespreksserver de oproep overdraagt.

Dit kan gebeuren in mobiele en afstandsbediening (MRA) en B2B oproepen.

Het kan geen geluid op één manier veroorzaken of een zoemend lawaai (het zelfde lawaai wanneer u probeert om een opname met gecodeerde audio te spelen) nadat de vraag wordt overgebracht. Dit gebeurt omdat een crypto suite geselecteerd is op aanroep die niet ondersteund wordt door het eindpunt waarop de suite wordt overgebracht.

U kunt de SIP-onderhandeling voor en na de overdracht van de oproep vergelijken. Bij de eerste onderhandeling in de VCS- of CUCM-logs kunt u cryptolijnen in het OK-bericht van 200 OK van VCS zien:

```
m=audio 54582 RTP/SAVP 9 96 97 0 8 18 101
a=rtpmap:9 G722/8000
a=rtpmap:96 G7221/16000
a=fmtp:96 bitrate=32000
a=rtpmap:97 G7221/16000
a=fmtp:97 bitrate=24000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:ckXijkT3CcVY+xlOf3ozX/TjHPz05OzEdY49rAHA|2^48
a=sendrecv
a=rtcp:54583 IN IP4 10.1.201.7
m=video 54658 RTP/SAVP 96 97
b=TIAS:4000000
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e01e;max-fs=1621;packetization-mode=1;max-rcmd-nalu-
size=32000;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42e01e;max-fs=1621;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:S8BJvGB/2l6F7XP8izXxId443Xd9f27oUI/4gxSt|2^48
```

Crypto lijnen worden geaccepteerd in de eerste oproep, maar in de tweede vraag zie je dat het ACK bericht de crypto lijnen verwijdert:

```
m=audio 24826 RTP/AVP 0
c=IN IP4 10.1.231.30
a=ptime:20
a=rtpmap:0 PCMU/8000
m=video 0 RTP/AVP 126
c=IN IP4 10.1.98.80
b=TIAS:448000
a=label:11
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42E01F;packetization-mode=1;max-fs=3601;max-rcmd-nalu-
size=32000;level-asymmetry-allowed=1
a=content:main
```

VCS probeert de crypto lijnen te gebruiken die in het begin zijn overeengekomen, zelfs als het eindpunt dat de vraag wordt overgebracht naar steunt geen encryptie.

Oplossing

Dit probleem heeft te maken met bug CSCuv1790

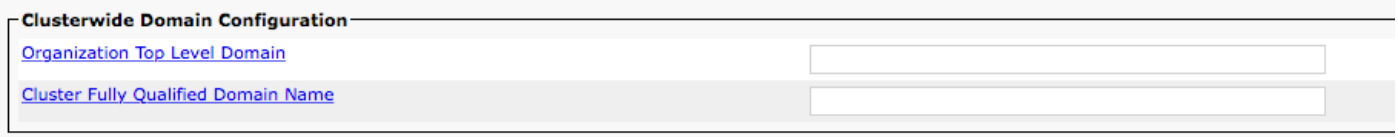
Upgradeautomaat VCS/Express naar x8.6.1 om dit probleem op te lossen.

3. Top Level Domain niet ingesteld in CUCM.

Als de Top Level Domain Enterprise Parameter niet is ingesteld, veroorzaakt het CUCM om inkomende oproepen naar zijn eigen domein te leiden en worden de SIP Routepatronen gebruikt. Dit zou een lus kunnen veroorzaken omdat de vraag zeer waarschijnlijk terug naar Exp-C wordt verzonden, of het kan ook met een "404 Not Found error" falen.

Oplossing

Van **CUCM Management-pagina navigeer naar System > Enterprise-parameters** om deze instelling te wijzigen



4. Het CUCM-certificaat moet van de clientverificatiekenmerken zijn voorzien.

Wanneer een beveiligde verbinding wordt ingesteld tussen de Exp-C en CUCM (TLS verify-encryptie) wordt de SSL-handdruk gestart door een specifieke callserver die afhankelijk is van de richting van de oproep. Dit betekent dat beide servers een client- en serververificatie moeten hebben in hun certificaten. Deze fout wordt in de VCS/Expressway-logbestanden gezien indien het kenmerk niet aanwezig is:

```
Line 190: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,060"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connecting"
Line 239: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,071"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Established"
Line 249: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,081"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Closed" Reason="no certificate returned"
```

Oplossing

Details over het configureren van een sjabloon met zowel webclient- als servereigenschappen zijn te vinden in de VCS-certificaatgids

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-7/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-7.pdf

5. Interworking-kwesties.

VCS/Expressway versie X8.6.x had een aantal problemen met het Interworking-proces.

Bogen in verband met het probleem:

Defect CSCuw85626 kan worden gedetecteerd als u de diagnostische logbestanden van VCS/Expressway controleert of videolijnen worden afgewezen:

Deze foutmelding wordt weergegeven wanneer de medielijnen in het TCS-gedeelte van de H323-stroom worden onderhandeld.

Medialine index: 1

verworpen: waar, richting: SDP_MEDIA_DIR_SENDRECV

type: Video / SDP_MF_AU_VID

Standaard CSCuw85715 is vergelijkbaar, maar in dit geval specificeren de VCS/Expressway-logboeken dat de oorzaak gegevensTypeNotOndersteuned is:

```
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="INFO": Action="Sent" Dst-ip="XXXXXXXXXXXXXXXX" Dst-port="49162"
Detail="Sending H.245 OpenLogicalChannelRejResponse "
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="DEBUG": Dst-ip="XXXXXXXXXXXXXXXX" Dst-port="49162"
Sending H.245 PDU:
value MultimediaSystemControlMessage ::= response : openLogicalChannelReject :
{
forwardLogicalChannelNumber 3,
cause dataTypeNotSupported : NULL
}
```

Oplossing

upgrade naar X8.7 of hoger.

6. ACK-bericht dat van CUCM is ontvangen, wordt niet naar VCS-E/Expressway-E verzonden.

Dit wordt meestal gezien wanneer de geconfigureerde traversal-zone niet op het juiste IP-adres van de VCS Expressway/Expressway-E wijst.

Bij één enkele NIC-implementaties (op de snelweg/contour-edge) moet de verplaatsen-clientzone op de Control/Core-instelling wijzen naar het openbare IP-adres van de traversale server.

Bij dubbele NIC-implementaties moet de overdrachtclient naar het interne IP-adres wijzen (interne NIC is meestal LAN1, maar kan LAN2 zijn) van de traversale server. Houd in gedachten dat dit het interne IP-adres van het interne LAN is.

Oplossing

Raadpleeg Bijlage 4 bij de Cisco VCS Express and VCS Control - Basic Configuration voor meer informatie en een schema van de verschillende netwerkimplementaties.

7. CUCM verlaagt TCP-sessie op inkomende oproepen

Wanneer oproepen vanuit VCS control/Expressway Core worden verzonden, kan CUCM dit verwerpen door de TCP sessie te laten vallen.

Dit kan gebeuren wanneer de haven tussen het buurgebied en het de veiligheidsprofiel van de boomstam van de lijn niet overeenkomt of gevormd wordt om 5060/5061 te zijn.

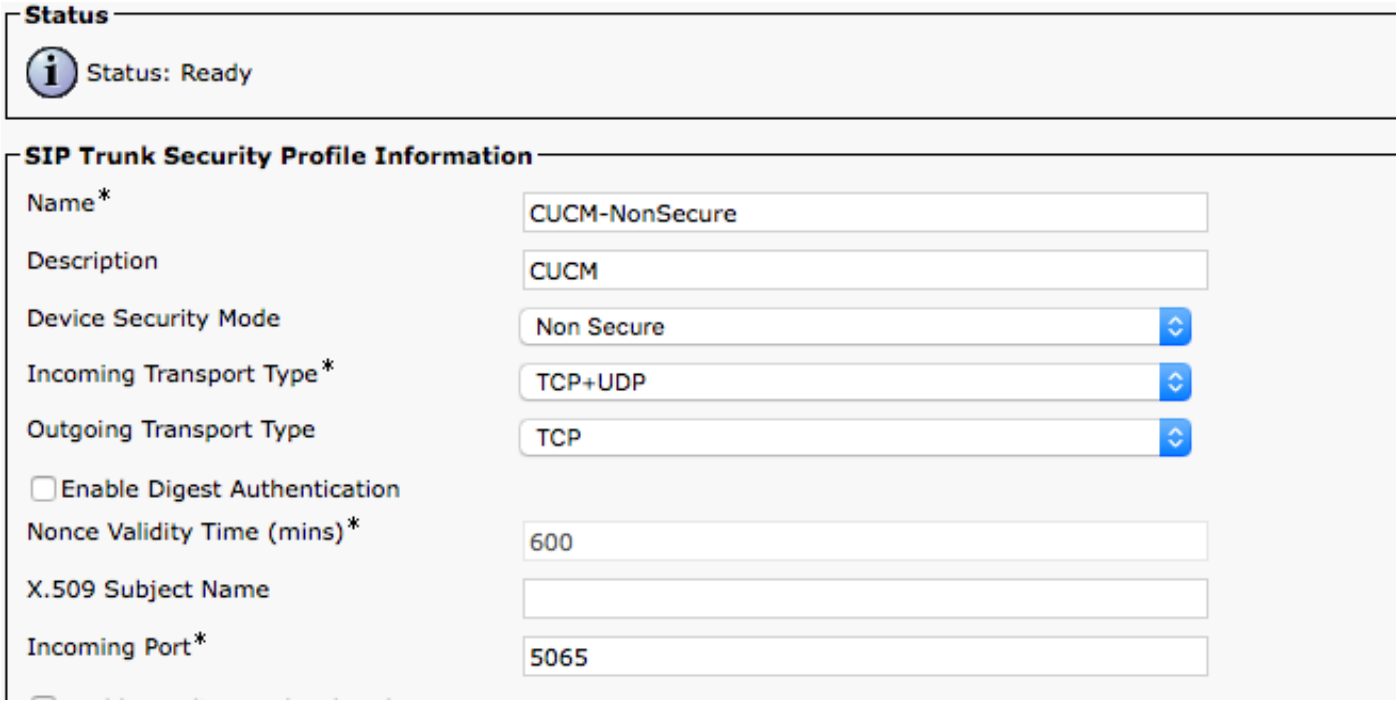
MRA gebruikt een inline-communicatie terwijl B2B-gesprekken een basiscommunicatie gebruiken, heeft CUCM een beperking die inline- en basiscommunicatie niet door dezelfde poort laat lopen. Omdat MRA meestal automatisch wordt geconfigureerd moeten B2B-implementaties een andere poort gebruiken.

Oplossing

Om dit te doen, moet de bestemmingshaven die op de buurzone naar CUCM (op VCS-C/Expressway-C) zijn geconfigureerd anders dan 5060/5061, normaal wordt 5065 gebruikt, maar andere kunnen worden gebruikt, moet de geconfigureerde poort overeenkomen met de poort in het SIP-torbeveiligingsprofiel dat aan deze server op CUCM is toegewezen.

Van **CUCM Management-pagina** navigeer **naar apparaat > Trunk.**

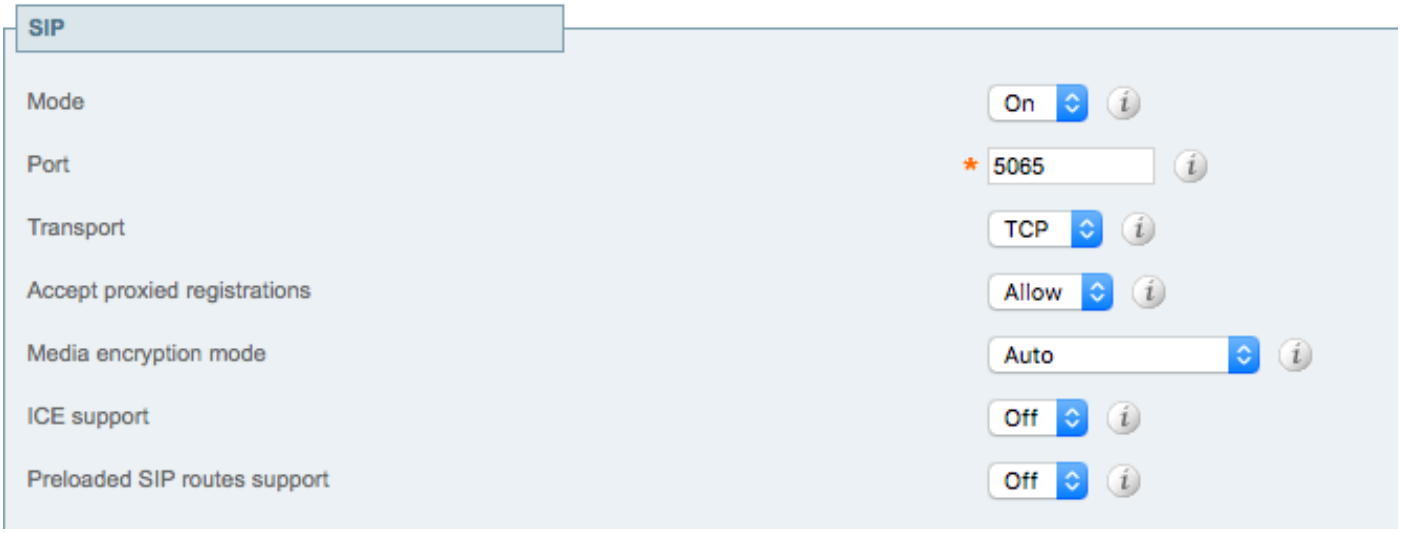
SIP Trunk-beveiligingsprofiel met poort 5065.



SIP Trunk-doelpoort kan 5060/5061 zijn, zoals in de afbeelding weergegeven.

SIP-poort in de buurzone VCS/Expressway moet overeenkomen met de poort die in het SIP Trunk-beveiligingsprofiel is geconfigureerd, zoals in de afbeelding.

Ga vanuit **de pagina** Snelheidsbeheer naar **Configuration > Protocols > SIP**



De VCS heeft deze beperking niet of is voor dit scenario niet van toepassing, wat betekent dat de SIP-stam zelf kan worden geconfigureerd met 5060/5061.

8. VCS kan geen FQDN's op de juiste wijze oplossen of geen SRV-records vragen.

Voor B2B-oproepen die afkomstig zijn van CUCM kan een probleem worden geïntroduceerd vanwege de aard van de wijze waarop CUCM oproepen en routeoproepen behandelt.

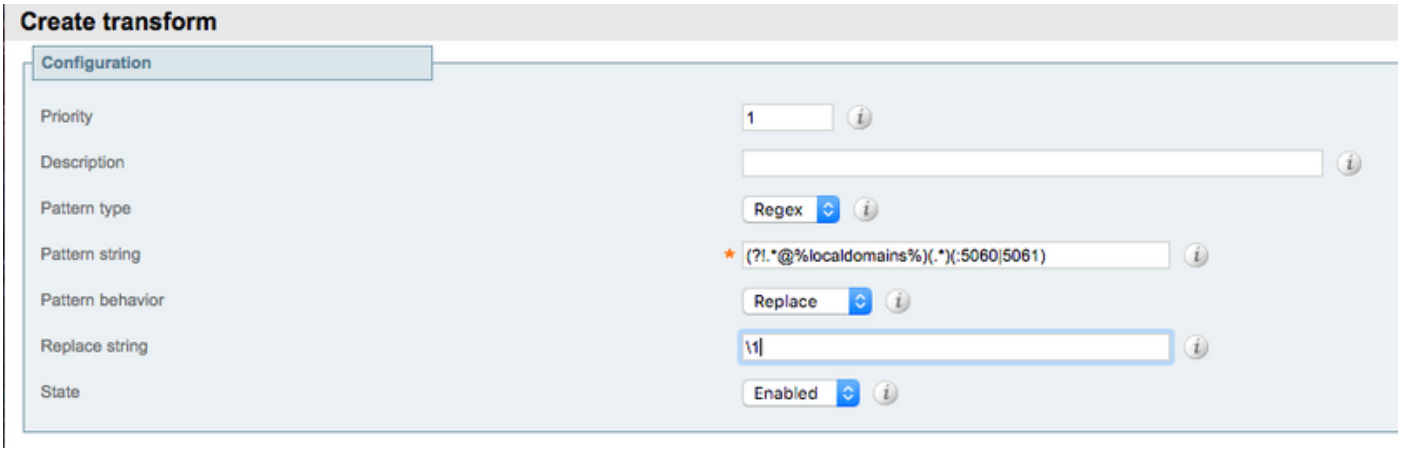
Wanneer CUCM-expediteur naar de VCS-servers belt, heeft CUCM de neiging 4:5060 of 4:5061 (afhankelijk van de configuratie) toe te voegen aan het einde van het URI-menu (d.w.z. test@lab.local > test@lab.local:5060) wanneer het de snelweg bereikt en een zoekregel naar de DNS-zone raakt, wordt er geen SRV-record gevraagd, maar alleen een reeks voor A of AAL AA records. U kunt dit bevestigen in de diagnostische logs van VCS/Expressway.

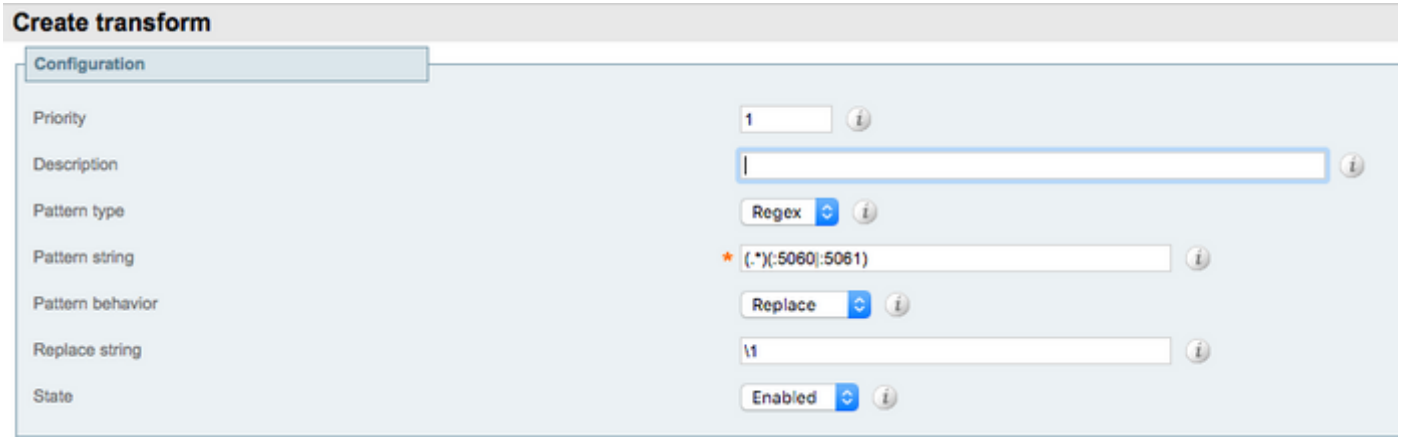
Oplossing

Om dit probleem op te lossen, creeer eenvoudig een transformatie die de poort aan het eind (op één van beide servers, het maakt niet echt uit) verwijdert voordat het de DNS zone bereikt.

Van **de pagina van het** Toezicht **van de Uitloop,** navigeer **Configuratie > Kiesschema > Configuratie omzetten > Kiesschema > Omzetten**

Omzet voorbeelden:





Als om de een of andere reden een transformatie niet kan worden gecreëerd, kan dit ook worden gedaan door middel van zoekregels, maar wordt aangeraden dit te doen door middel van transformaties.

Van **pagina** voor **directie van snelwegen,** navigeer **naar configuratie > Kiesschema > Omzetten > Kiesschema > Zoeken regels**

Gerelateerde informatie

- Cisco VCS Express en VCS-controle - basisconfiguratie