Verwenden Sie NAT, um die tatsächliche IP-Adresse der ONS 15454 auszublenden, um eine CTC-Sitzung einzurichten.

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Topologie
Konfiguration
Netzwerkdiagramm
Konfigurationen
Konfiguration von Cisco ONS 15454
Konfiguration des Computers
Routerkonfiguration
Überprüfung
Überprüfungsverfahren
Fehlerbehebung
Zugehörige Informationen

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für Network Address Translation (NAT), um eine Sitzung zwischen dem Cisco Transport Controller (CTC) und ONS 15454 einzurichten. Die Konfiguration verwendet NAT und eine Zugriffsliste, wenn sich die ONS 15454 in einem privaten Netzwerk und der CTC-Client in einem öffentlichen Netzwerk befindet.

Wenden Sie NAT und eine Zugriffsliste aus Sicherheitsgründen an. NAT verbirgt die tatsächliche IP-Adresse von ONS 15454. Die Zugriffsliste dient als Firewall zur Steuerung des IP-Datenverkehrs innerhalb und außerhalb der ONS 15454.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Grundkenntnisse der Cisco ONS 15454
- Beachten Sie, welche Cisco Router NAT unterstützen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS® Softwareversion 12.1(11) und höher
- Cisco ONS 15454 Version 5.X und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Dieser Abschnitt enthält die wichtigsten Hintergrundinformationen.

Topologie

Die Testtopologie umfasst:

- Eine Cisco ONS 15454, die als Server fungiert.
- Ein PC dient als CTC-Client.
- Ein Cisco Router der Serie 2600 mit NAT-Unterstützung.

Hinweis: Cisco ONS 15454 ist im internen Netzwerk und der PC im externen Netzwerk installiert.

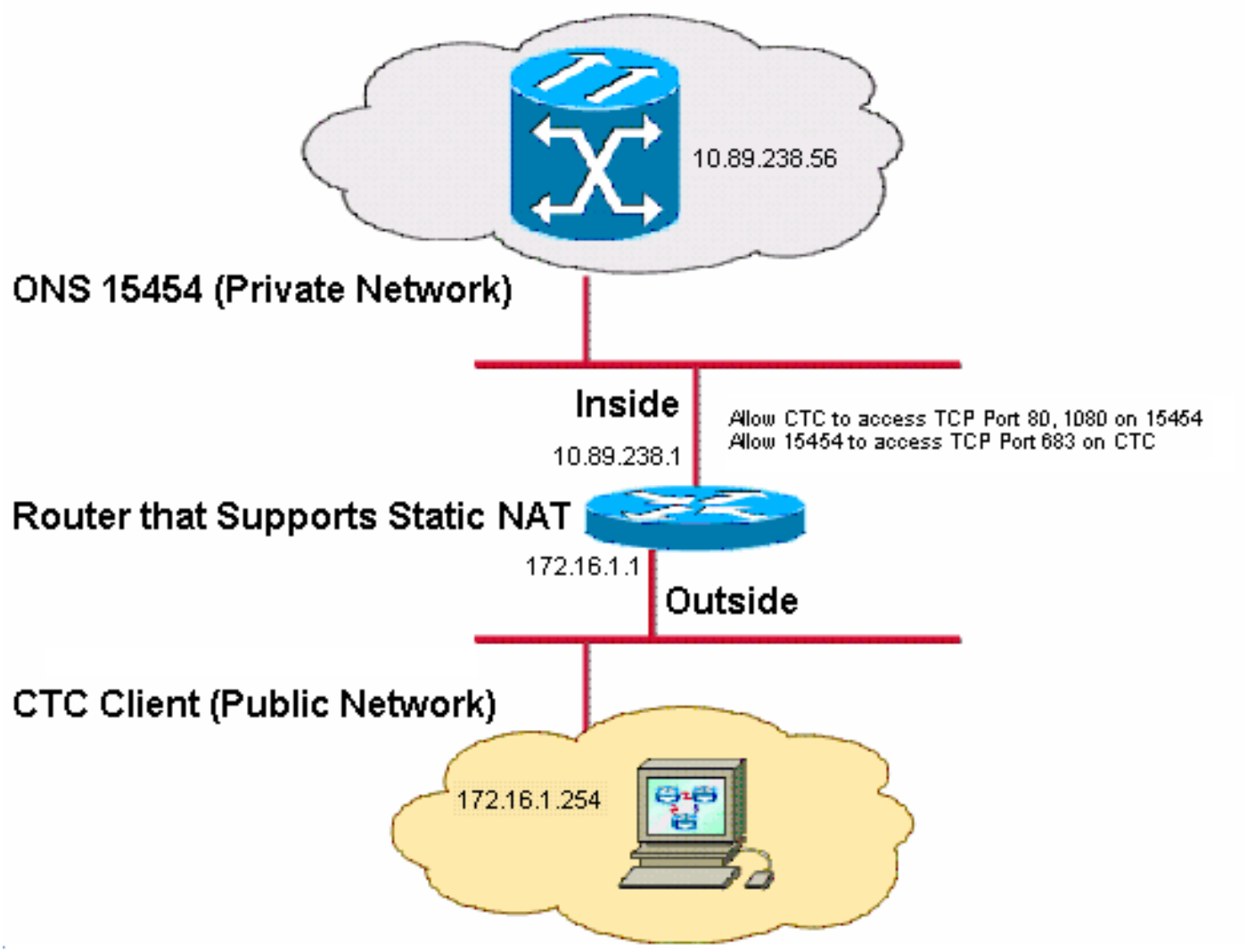
Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Nehmen Sie an, dass 172.16.0.0 im öffentlichen Netzwerk routbar ist.

Konfigurationen

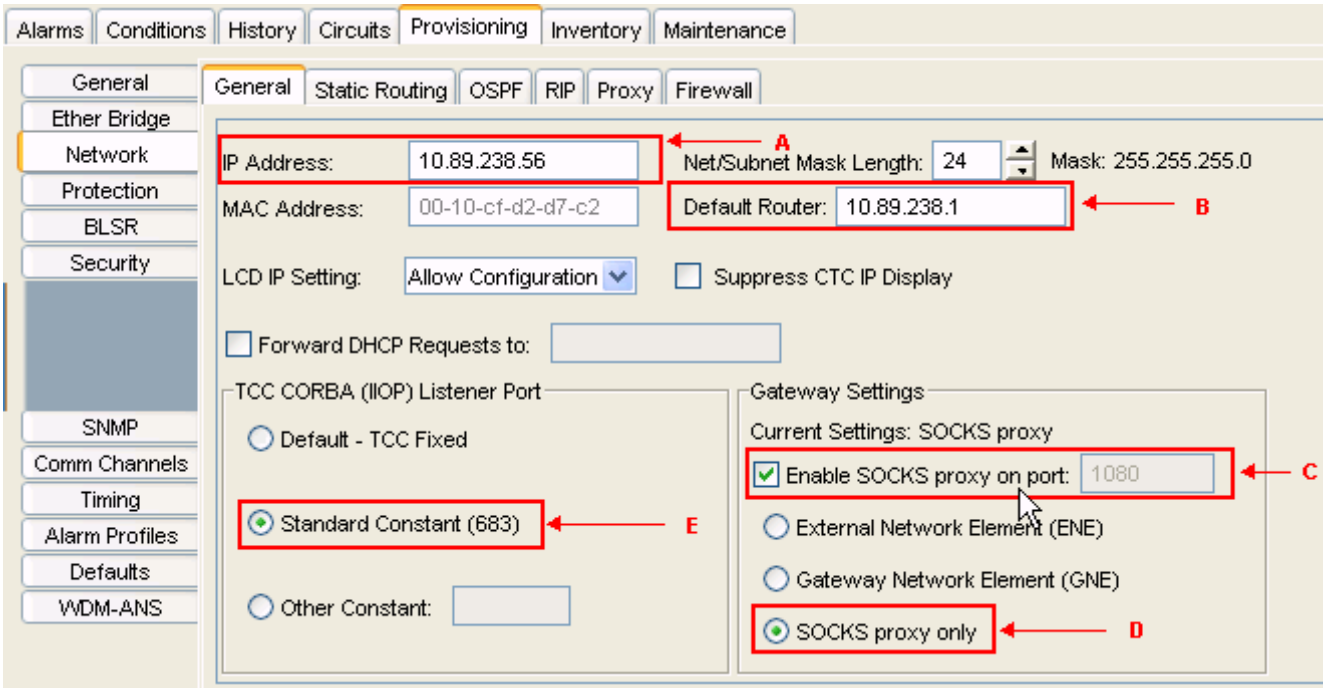
In diesem Dokument werden folgende Konfigurationen verwendet:

- ONS 15454
- PC
- Router

Konfiguration von Cisco ONS 15454

Führen Sie diese Schritte aus:

1. Klicken Sie in der Knotenansicht auf **Provisioning > General > Network (Bereitstellung > Allgemein > Netzwerk)**.Überprüfen Sie, ob die IP-Adresse des ONS 15454 im Feld "IP Address" (IP-Adresse) als 10.89.238.56 angezeigt wird (siehe Pfeil A in Abbildung 2) und dass das Feld Default Router den Wert 10.89.238.1 enthält (siehe Pfeil B in Abbildung 2).**Abbildung 2: Konfiguration von ONS 15454**

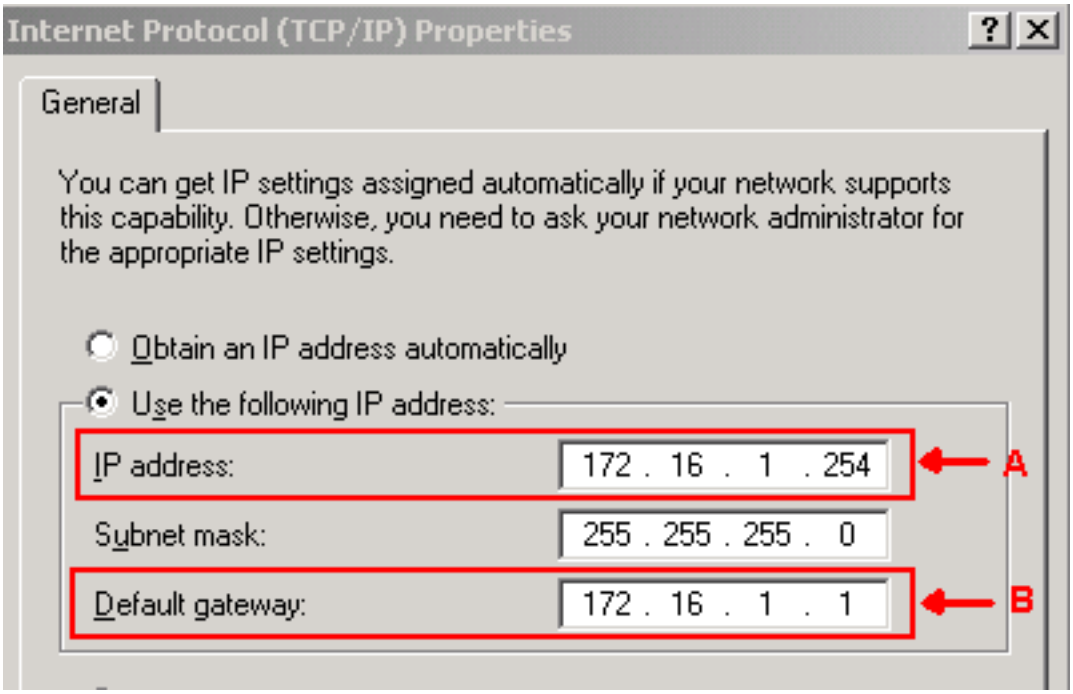


2. Aktivieren Sie das Kontrollkästchen **SOCKS-Proxy am Port aktivieren** im Abschnitt Gateway-Einstellungen (siehe Pfeil C in Abbildung 2), und wählen Sie die Option **SOCKS-Proxy** (siehe Pfeil D in Abbildung 2).
3. Wählen Sie die gewünschte Listener-Port-Option im Abschnitt TCC CORBA (IIOP) Listener Port aus. Sie haben die folgenden drei Optionen:**Standard - TCC Fixed** (Standard - TCC-**fest**) - Wählen Sie diese Option aus, wenn sich der ONS 15454 auf derselben Seite der Firewall wie der CTC-Computer befindet oder wenn keine Firewall vorhanden ist (Standard). Diese Option legt den ONS 15454-Listener-Port auf Port 57790 fest. Wenn Port 5790 geöffnet ist, können Sie die Option Default - TCC Fixed für den Zugriff über eine Firewall verwenden.**Standard Constant (Standardkonstante)**: Wählen Sie diese Option aus, um Port 683, die CORBA-Standardportnummer, als den ONS 15454-Listener-Port zu verwenden. In diesem Beispiel wird Standard Constant (683) verwendet (siehe Pfeil E in Abbildung 2).**Other Constant (Andere Konstante)**: Wählen Sie diese Option aus, wenn Sie Port 683 nicht verwenden. Geben Sie den IIOP-Port ein, den Ihr Firewall-Administrator angibt.

Konfiguration des Computers

Überprüfen Sie im Dialogfeld Eigenschaften von Internetprotokoll (TCP/IP), ob im Feld IP-Adresse 172.16.1.254 als IP-Adresse des PCs angegeben ist (siehe Pfeil A in Abbildung 3). Überprüfen Sie außerdem, ob 172.16.1.1 das Standardgateway ist (siehe Pfeil B in Abbildung 3).

Abbildung 3: PC-Konfiguration



Routerkonfiguration

Führen Sie diese Schritte aus:

1. Konfigurieren Sie die interne Schnittstelle, in der sich die Cisco ONS 15454 befindet.
```
!
interface Ethernet1/0
 ip address 10.89.238.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
!
```
2. Konfigurieren Sie die Zugriffsliste 101.
```
access-list 101 permit tcp any eq www any
!
! Allow CTC to access TCP Port 80 on ONS 15454
!
access-list 101 permit tcp any eq 1080 any
!
! Allow CTC to access TCP Port 1080 on ONS 15454
!
access-list 101 permit tcp any any eq 683
!
! Allow ONS 15454 to access TCP Port 683 on the PC
!
```
3. Konfigurieren Sie die externe Schnittstelle, auf der sich der PC befindet.
```
interface Ethernet1/1
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
!
```
4. Konfigurieren Sie statische NAT.Die Konfiguration wandelt die IP-Adresse 10.89.238.56 (intern lokal) in die IP-Adresse 172.16.1.200 (außerhalb global) um. Geben Sie den Befehl **show ip nat translation** auf dem Router ein, um die Übersetzungstabelle anzuzeigen (siehe Abbildung 4).
```
!
ip nat inside source static 10.89.238.56 172.16.1.200
!
```
Abbildung 4: IP NAT Translation

```
2600-4#show ip nat translation
Pro Inside global  Inside local  Outside local  Outside global
--- 172.16.1.200   10.89.238.56  ---            ---
```

Überprüfung

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs **show abrufen lassen.**

- **show access-list**: Zeigt die Anzahl der Pakete an, die die Zugriffsliste passieren.

Überprüfungsverfahren

Gehen Sie wie folgt vor, um die Konfiguration zu überprüfen:

1. Führen Sie Microsoft Internet Explorer aus.
2. Geben Sie **http://172.16.1.200** im Adressfeld des Browserfensters ein, und drücken Sie die EINGABETASTE.172.16.1.200 ist die interne globale Adresse. Im öffentlichen Netzwerk können CTC-Benutzer nur auf 172.16.1.200 zugreifen. Dies ist die interne globale Adresse der ONS 15454, deren interne lokale Adresse 10.89.238.56 lautet.Das Fenster CTC-Anmeldung wird angezeigt.
3. Geben Sie den Benutzernamen und das Kennwort ein, um sich anzumelden.Der CTC-Client stellt erfolgreich eine Verbindung zur ONS 15454 her.
4. Geben Sie den Befehl **debug ip nat detail** ein, um die detaillierte IP NAT-Verfolgung zu aktivieren. Sie können die Adressübersetzungen in der Ablaufverfolgungsdatei anzeigen. Beispiel: Adressumwandlung von 10.89.238.56 bis 172.16.1.200 (siehe Pfeil A in Abbildung 5) und von 172.16.1.200 bis 10.89.238.56 (siehe Pfeil B in Abbildung 5).**Abbildung 5: Detailliertes Debuggen der IP NAT**

```
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55499]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55499]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55500]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55500]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55501]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32895]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32895]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32897]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32897]
```

A

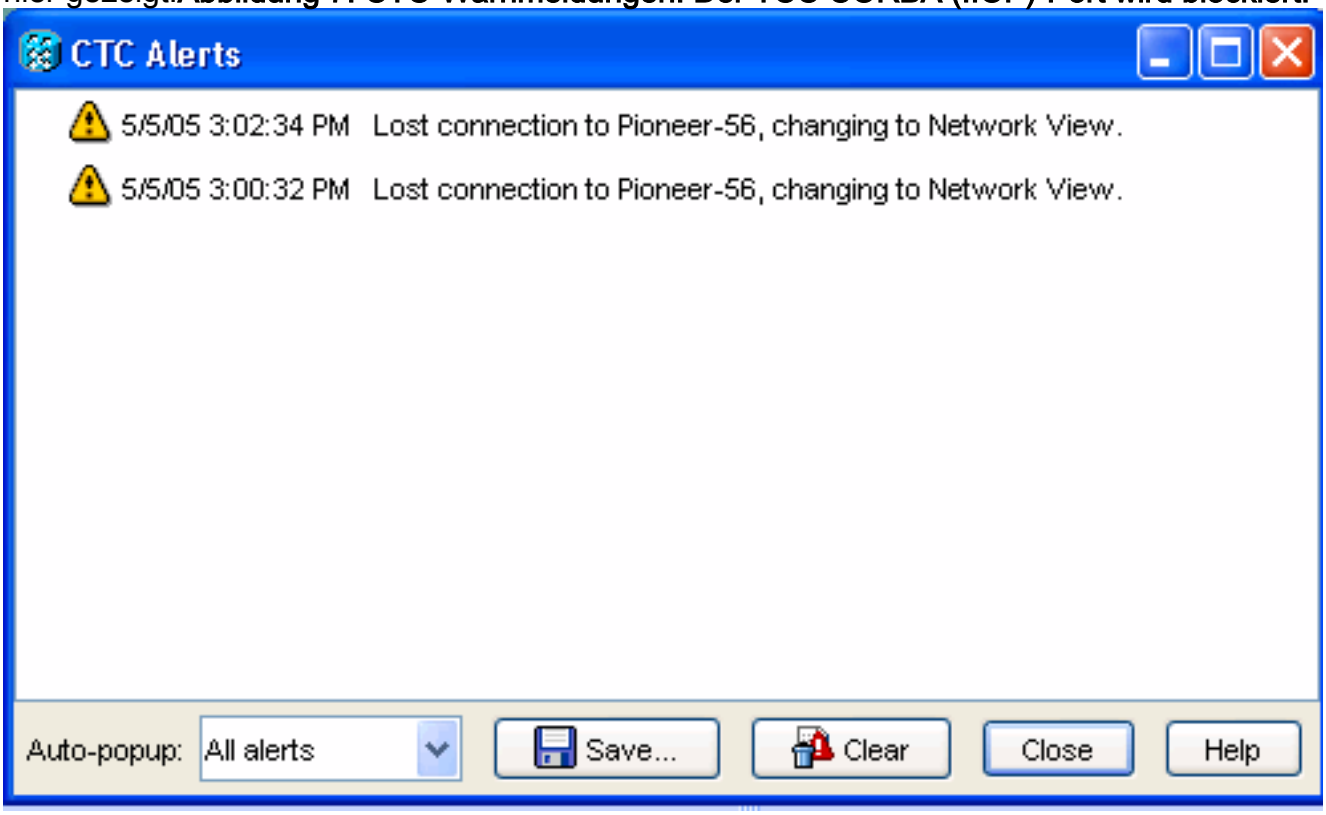
B

5. Geben Sie den Befehl **access-list (Zugriffsliste) auf** dem Router ein, um die Anzahl der Pakete anzuzeigen, die die Zugriffsliste durchlaufen.**Abbildung 6: Befehl show access-list**

```
2600-4#show access-list
Extended IP access list 101
    permit tcp any eq www any (56 matches)
    permit tcp any eq 1080 any (330 matches)
    permit tcp any any eq 683 (6 matches)
```

Wenn

die Zugriffsliste den TCC CORBA (IIOP) Listener Port blockiert, tritt die CTC-Sitzung mit der ONS 15454 regelmäßig ein, und alle zwei Minuten wird eine Warnmeldung angezeigt, wie hier gezeigt:**Abbildung 7: CTC-Warnmeldungen: Der TCC CORBA (IIOP)-Port wird blockiert.**



Als Problemumgehung können Sie den CTC IIOP-Listener-Port öffnen. Cisco Bug ID CSCeh96275 (nur registrierte Kunden) behebt dieses Problem.Künftig reicht die Einrichtung eines Kabelrohrs für TCP-Ports 80 und 1080 auf der Firewall aus, um die tatsächliche IP-Adresse der ONS 15454 zu verbergen.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme