Use NAT to Hide the Real IP Address of ONS 15454 to Establish a CTC Session

Document ID: 64816

Contents

Introduction

This document provides a sample configuration for Network Address Translation (NAT) to establish a session between Cisco Transport Controller (CTC) and ONS 15454. The configuration uses NAT and an access list when the ONS 15454 resides in a private network, and the CTC client resides in a public network.

Apply NAT and an access list for security purposes. NAT hides the real IP address of ONS 15454. The access list serves as a firewall to control the IP traffic in and out of the ONS 15454.

Prerequisites

Requirements

Before you attempt this configuration, ensure that you meet these requirements:

- Have basic knowledge of Cisco ONS 15454.
- Be aware of which Cisco Routers support NAT.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software Release 12.1(11) and later
- Cisco ONS 15454 version 5.X and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

This section provides the essential background information.

Topology

The test topology comprises:

- One Cisco ONS 15454, which acts as the server.
- One PC, which serves as the CTC client.
- One Cisco 2600 series router, which provides the NAT support.

Note: Cisco ONS 15454 resides in the internal network and the PC is in the external network.

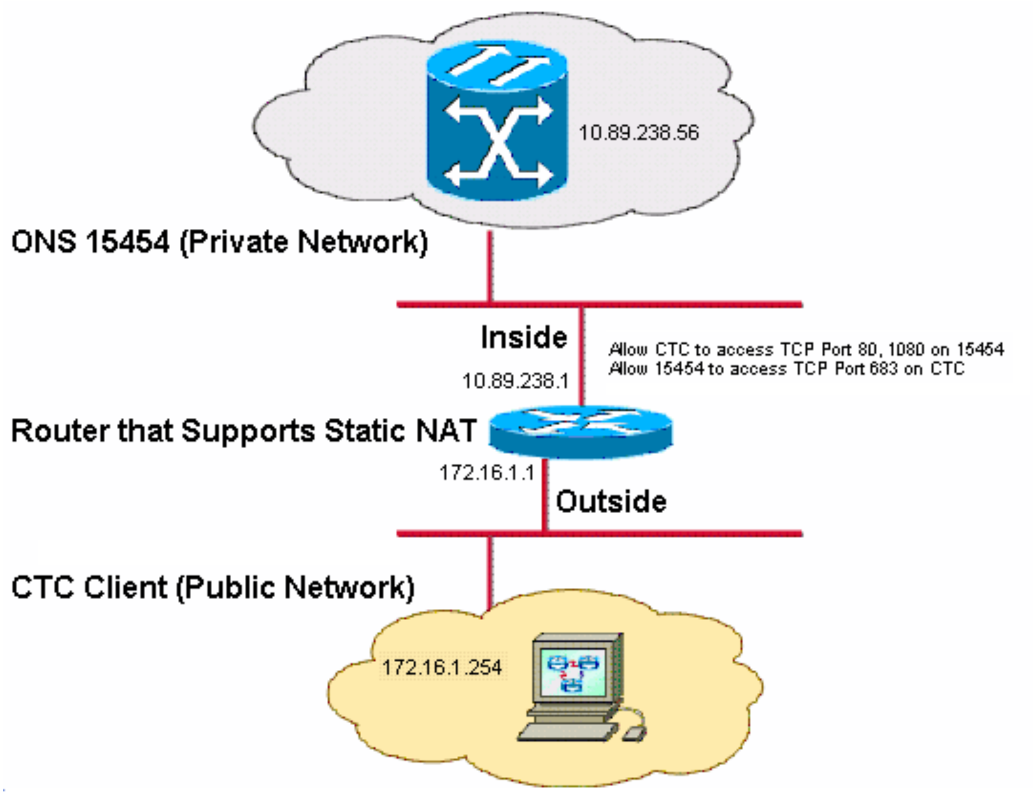
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:


10.89.238.56
ONS 15454 (Private Network)
Inside
Allow CTC to access TCP Port 80, 1080 on 15454
Allow 15454 to access TCP Port 683 on CTC
10.89.238.1
Router that Supports Static NAT
172.16.1.1
Outside
CTC Client (Public Network)
172.16.1.254

Note: Assume that 172.16.0.0 is routable in the public network.

Configurations

This document uses these configurations:

- ONS 15454
- PC
- Router

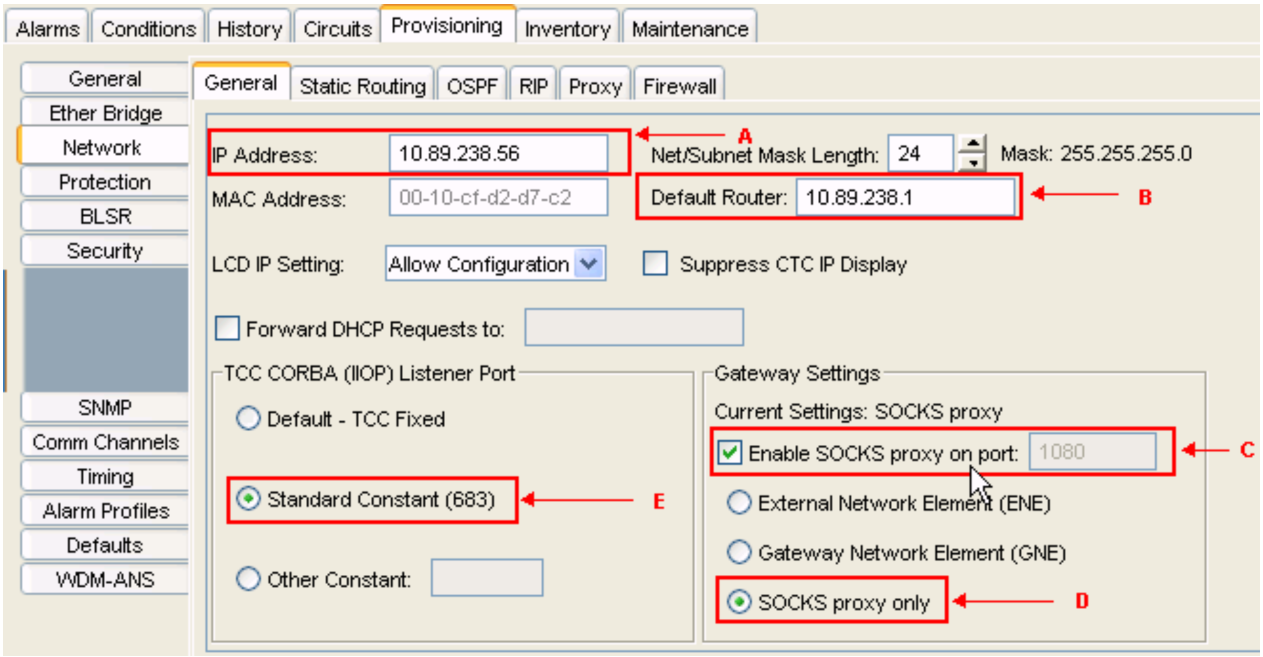
Cisco ONS 15454 Configuration

Complete these steps:

1. In the node view, click **Provisioning > General > Network**.

   Verify whether the IP address of the ONS 15454 appears as 10.89.238.56 in the IP Address field (see arrow A in Figure 2), and that the Default Router field contains the value 10.89.238.1 (see arrow B in Figure 2).

   Figure 2 ONS 15454 Configuration



IP Address: 10.89.238.56

Net/Subnet Mask Length: 24

Mask: 255.255.255.0

MAC Address: 00-10-cf-d2-d7-c2

Default Router: 10.89.238.1

LCD IP Setting: Allow Configuration

□ Suppress CTC IP Display

□ Forward DHCP Requests to:

TCC CORBA (IIOP) Listener Port

○ Default - TCC Fixed

● Standard Constant (683)

○ Other Constant:

Gateway Settings

Current Settings: SOCKS proxy

☑ Enable SOCKS proxy on port: 1080

○ External Network Element (ENE)

○ Gateway Network Element (GNE)

● SOCKS proxy only

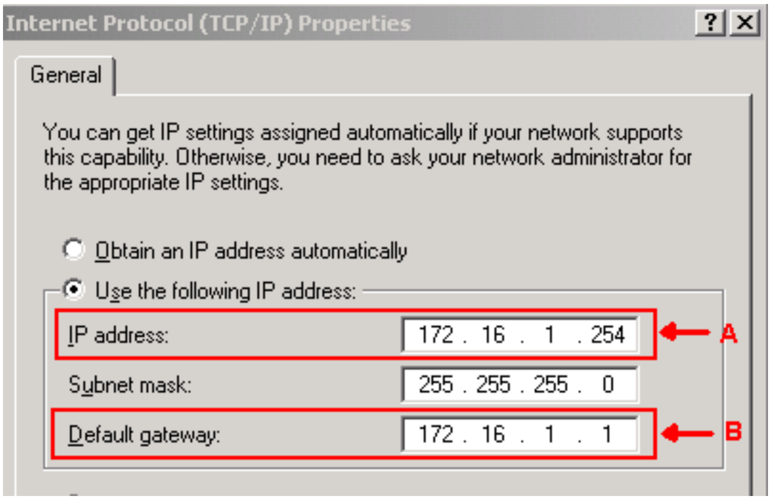
2. Check the **Enable SOCKS proxy on port** check box in the Gateway Settings section (see arrow C in Figure 2), and select the **SOCKS proxy only** option (see arrow D in Figure 2).
3. Select the required listener port option in the TCC CORBA (IIOP) Listener Port section. You have these three options:

   - **Default − TCC Fixed** Select this option if the ONS 15454 is on the same side of the firewall as the CTC computer, or if there is no firewall (default). This option sets the ONS 15454 listener port to Port 57790. You can use the Default − TCC Fixed option for access through a firewall if Port 57790 is open.
   - **Standard Constant** Select this option to use Port 683, the CORBA default port number, as the ONS 15454 listener port. This example uses Standard Constant (683) (see arrow E in Figure 2).
   - **Other Constant** Select this option if you do not use Port 683. Type the IIOP port that your firewall administrator specifies.

Personal Computer Configuration

In the Internet Protocol (TCP/IP) Properties dialog box, verify whether the IP address field indicates 172.16.1.254 as the IP address of the PC (see arrow A in Figure 3). Also check whether 172.16.1.1 is the default gateway (see arrow B in Figure 3).

Figure 3   PC Configuration



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 16 . 1 . 254

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 1 . 1

Router Configuration

Complete these steps:

1. Configure the inside interface where Cisco ONS 15454 resides.

```
!
interface Ethernet1/0
 ip address 10.89.238.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
!
```

2. Configure access− list 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. Configure the outside interface where the PC resides.

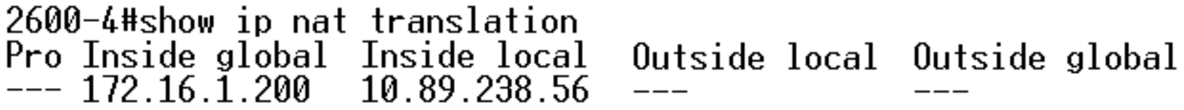
```
interface Ethernet1/1
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
!
```

4. Configure static NAT.

   The configuration converts the IP address of 10.89.238.56 (inside local) to the IP address of 172.16.1.200 (outside global). Issue the **show ip nat translation** command on the router to view the translation table (see Figure 4).

```
!
ip nat inside source static 10.89.238.56 172.16.1.200
!
```

Figure 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    ---             ---
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show access−list** displays the count of packets that pass through the access list.

Verification Procedure

Complete these steps to verify the configuration:

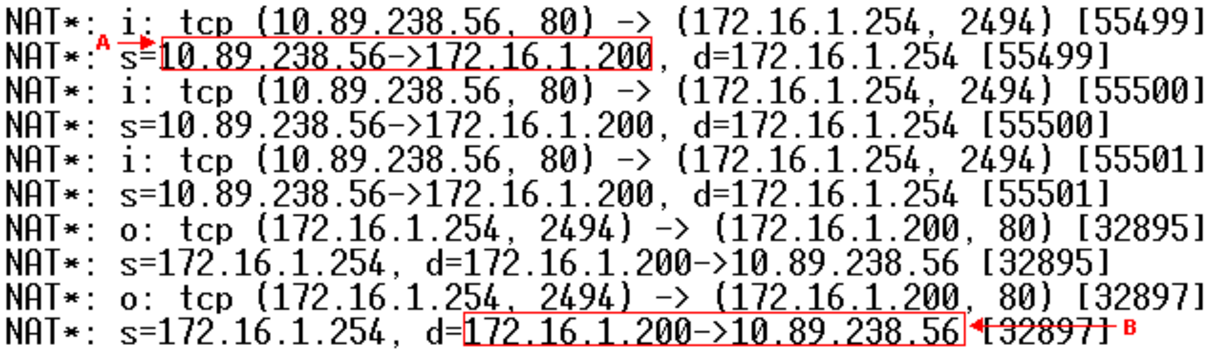
1. Run Microsoft Internet Explorer.
2. Type **http://172.16.1.200** in the Address field of the browser window, and press ENTER.

   172.16.1.200 is the inside global address. In the public network, CTC users can access only 172.16.1.200, which is the inside global address of the ONS 15454 whose inside local address is 10.89.238.56.

   The CTC Login window appears.
3. Type the user name and password to log in.

   The CTC client successfully connects to the ONS 15454.
4. Issue the **debug ip nat detailed** command to turn on the IP NAT detailed trace. You can view the address translations in the trace file. For example, address translation from 10.89.238.56 to 172.16.1.200 (see arrow A in Figure 5), and from 172.16.1.200 to 10.89.238.56 (see arrow B in Figure 5).

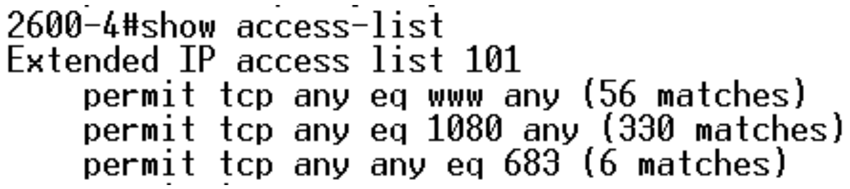
   Figure 5   Debug IP NAT Detailed

```
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]
```

5. Issue **show access−list** command on the router to view the count of packets that pass through the access list.

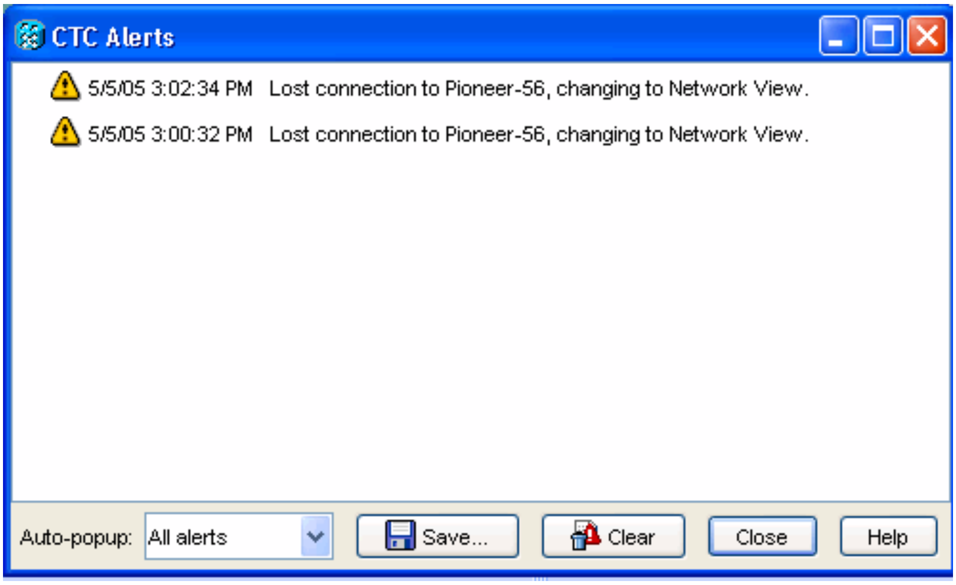
   Figure 6   The show access−list Command



```
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)
```

If the access list blocks the TCC CORBA (IIOP) Listener Port, the CTC session with the ONS 15454 times out regularly, and an alert message appears every two minutes as shown here:

Figure 7 CTC Alerts: The TCC CORBA (IIOP) Port is Blocked



⚠ 5/5/05 3:02:34 PM Lost connection to Pioneer-56, changing to Network View.
⚠ 5/5/05 3:00:32 PM Lost connection to Pioneer-56, changing to Network View.

Auto-popup: All alerts

As a workaround, you can open the CTC IIOP listener port. Cisco bug ID CSCeh96275 (registered customers only) addresses this issue.

In the future, creation of a conduit for TCP Port 80 and 1080 on the firewall is enough to provide support to hide the real IP address of ONS 15454.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation − Cisco Systems**