

ONS 15454 の実際の IP アドレスを隠すために、CTC セッションの確立に NAT を使用

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[トポロジ](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[Cisco ONS 15454 の設定](#)

[パーソナル コンピュータの設定](#)

[ルータの設定](#)

[確認](#)

[確認手順](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Transport Controller (CTC) と ONS 15454 間にセッションを確立するためのネットワーク アドレス変換 (NAT) の設定例を紹介します。この設定は、ONS 15454 がプライベート ネットワークにあり、CTC クライアントがパブリック ネットワークにある場合、NAT とアクセス リストを使用します。

NAT とアクセス リストはセキュリティ上の理由で適用します。NAT は ONS 15454 の実際の IP アドレスを隠します。アクセス リストはファイアウォールとして ONS 15454 を出入りして IP トラフィックを制御するのに動作します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- Cisco ONS 15454 についての基本的な知識がある。
- どの Cisco ルータで NAT がサポートされているかを把握している。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS(R) ソフトウェア リリース 12.1(11) 以降
- Cisco ONS 15454 バージョン 5.X 以降

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

このセクションには、重要な背景情報を記載します。

トポロジ

テスト トポロジは次の要素で構成されています。

- Cisco ONS 15454 : 1 台 (サーバとして機能)
- PC : 1 台 (CTC クライアントとして機能)
- Cisco 2600 シリーズ ルータ : 1 台 (NAT サポートを提供)

注: Cisco ONS 15454 は内部ネットワーク上にあり、PC は外部ネットワーク上にあります。

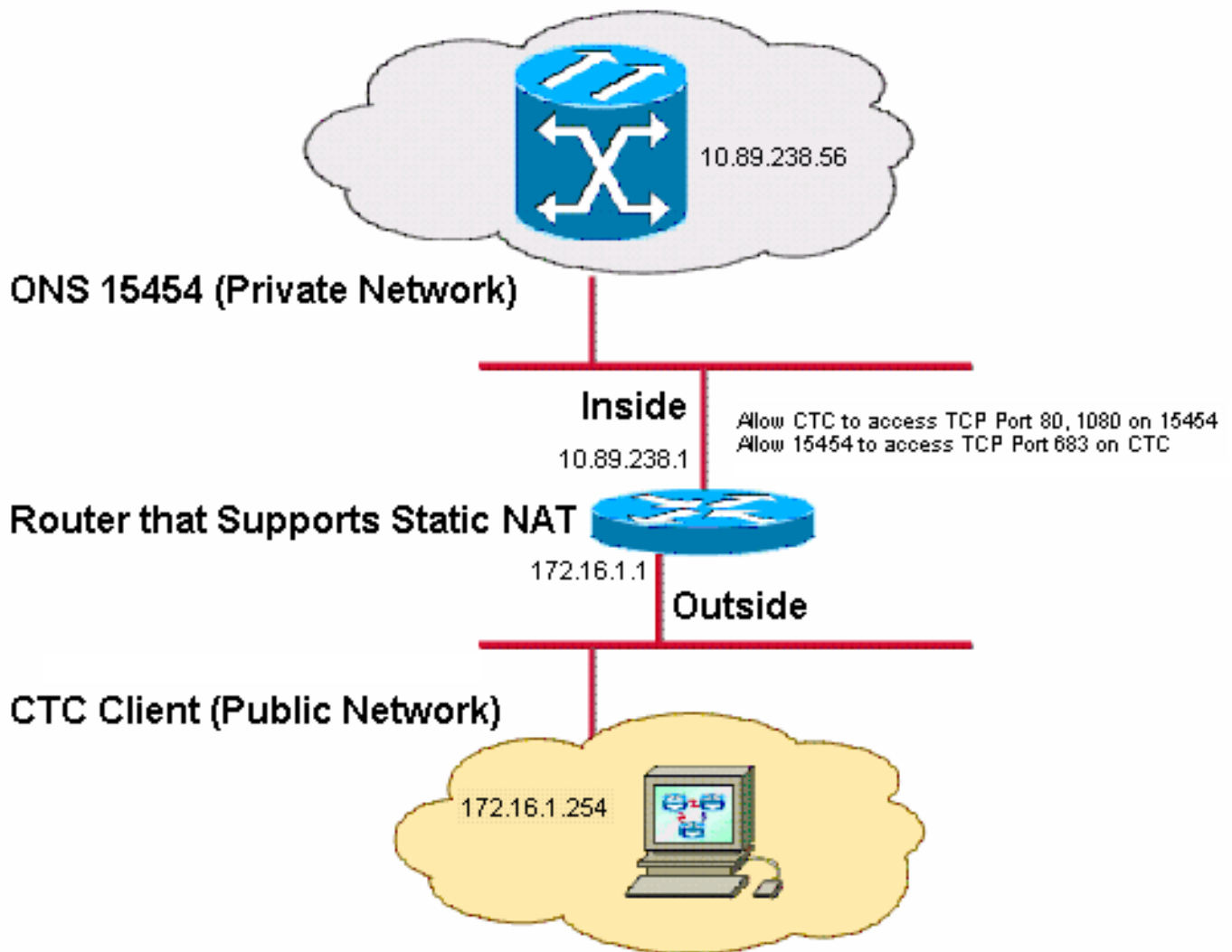
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: 172.16.0.0 はパブリック ネットワーク内でルーティング可能という前提です。

設定

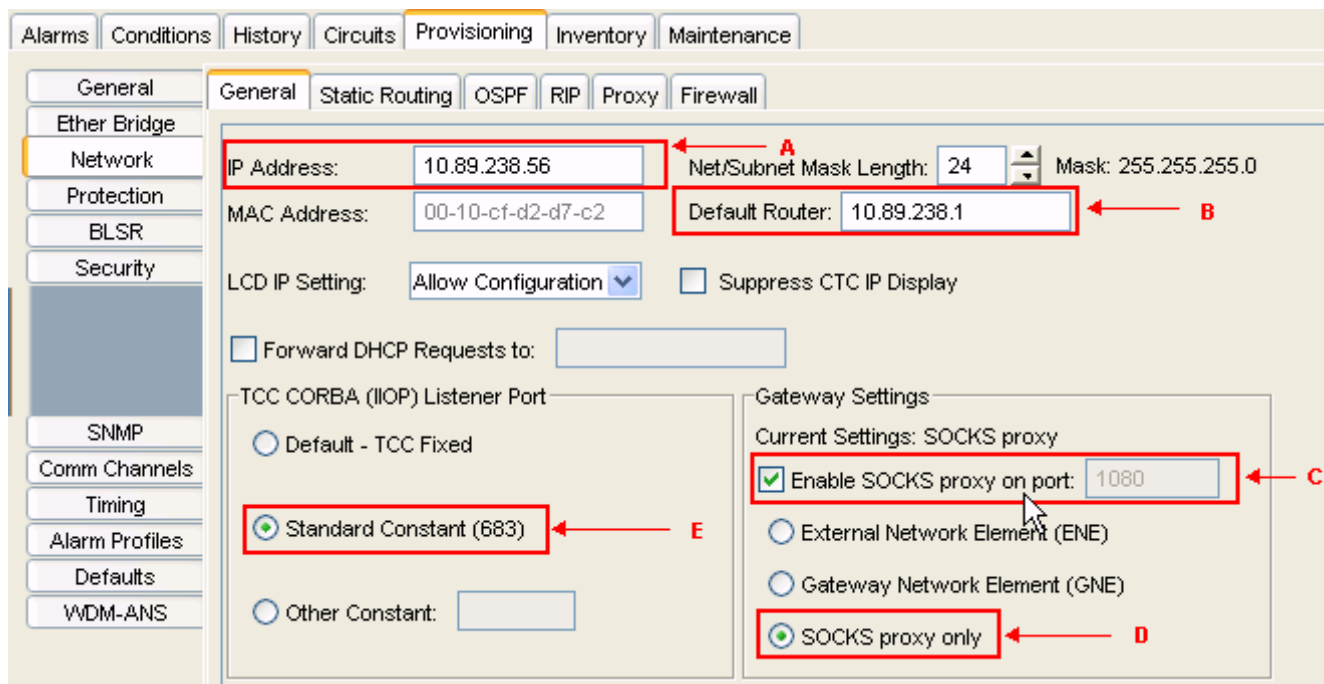
このドキュメントでは、次の設定を使用します。

- ONS 15454
- PC
- ルータ

Cisco ONS 15454 の設定

次の手順を実行します。

1. Node View では、Provisioning > General > Network の順にクリックして下さい。IP Address フィールドに ONS 15454 の IP アドレスとして 10.89.238.56 ([図 2](#) の矢印 A を参照) と表示され、Default Router フィールドに 10.89.238.1 ([図 2](#) の矢印 B を参照) と表示されていることを確認します。 **図 2 – ONS 15454 設定**

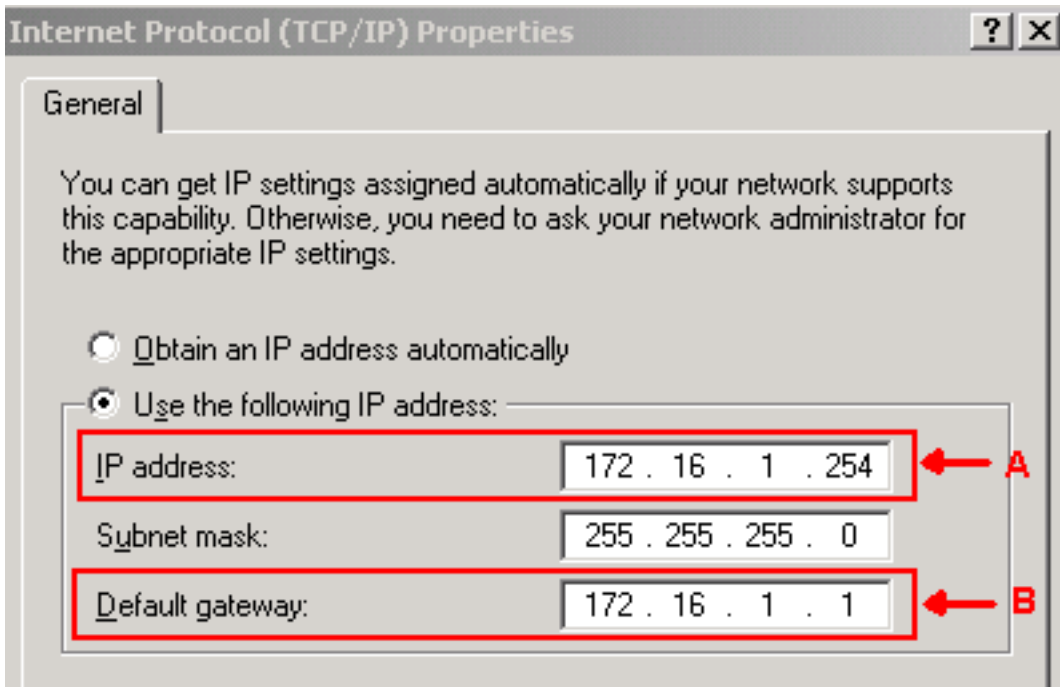


- Gateway Settings のセクションで Enable SOCKS proxy on port チェックボックスにチェックマークを付け (図 2 の矢印 C を参照)、SOCKS proxy only オプション (図 2 の矢印 D を参照) を選択します。
- TCC CORBA (IIO) Listener Port セクションで、適切なリスナー ポート オプションを選択します。次の 3 つのオプションがあります。デフォルト-固定される TCC — ONS 15454 が CTC コンピュータとファイアウォールの同じ側にあるか、またはファイアウォール (デフォルト) がなかったらこのオプションを選択して下さい。オプションが設定 ONS 15454 リスナー ポート ポート 57790 にこの。デフォルト使用できます- TCC はファイアウォールによってポート 57790 が開いている場合アクセスのためのオプションを固定しました。標準定数— ONS 15454 リスナー ポートとしてポート 683 を、CORBA デフォルトポート数、使用するこのオプションを選択して下さい。この例では Standard Constant (683) (図 2 の矢印 E を参照) を使用します。他の定数—ポート 683 を使用しない場合このオプションを選択して下さい。ファイアウォールの 管理者が規定する IIO) ポートを入力して下さい。

パーソナルコンピュータの設定

Internet Protocol (TCP/IP) Properties ダイアログボックスで、PC の IP アドレスとして IP address フィールドに 172.16.1.254 と表示されていることを確認します (図 3 の矢印 A を参照)。また、デフォルト ゲートウェイが 172.16.1.1 になっていることを確認します (図 3 の矢印 B を参照)。

図 3 – PC 設定



ルータの設定

次の手順を実行します。

1. Cisco ONS 15454 が存在する内部インターフェイスを設定します。!

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

2. access- list 101 を設定します。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 80 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. PC が存在する外部インターフェイスを設定します。interface Ethernet1/1

```
ip address 172.16.1.1 255.255.255.0
ip nat outside
!
```

4. 静的 NAT を設定します。この設定により、IP アドレス 10.89.238.56 (内部ローカル) が IP アドレス 172.16.1.200 (外部グローバル) に変換されます。ルータで show ip nat translation コマンドを発行すると、変換テーブルを表示できます ([図4](#) を参照) 。!

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

! **図4 - IP Nat変換**

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

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の show コマンドは、[Output Interpreter Tool](#) (登録ユーザ専用) によってサポートされています。このツールを使用すると、show コマンド出力の分析を表示できます。

- show access-list — パススルー アクセス リスト パケットのカウンタを表示する。

確認手順

次の手順を実行して設定を確認します。

1. Microsoft Internet Explorer を起動します。
2. ブラウザ ウィンドウのアドレス フィールドに http://172.16.1.200 と入力し、Enter キーを押します。172.16.1.200 は内部グローバル アドレスです。パブリック ネットワークで CTC ユーザがアクセスできるのは 172.16.1.200 だけです。これは、内部ローカル アドレスが 10.89.238.56 である ONS 15454 の内部グローバル アドレスです。CTC ログイン ウィンドウが表示されます。
3. ユーザ名とパスワードを入力してログインします。CTC クライアントが ONS 15454 との接続に成功します。

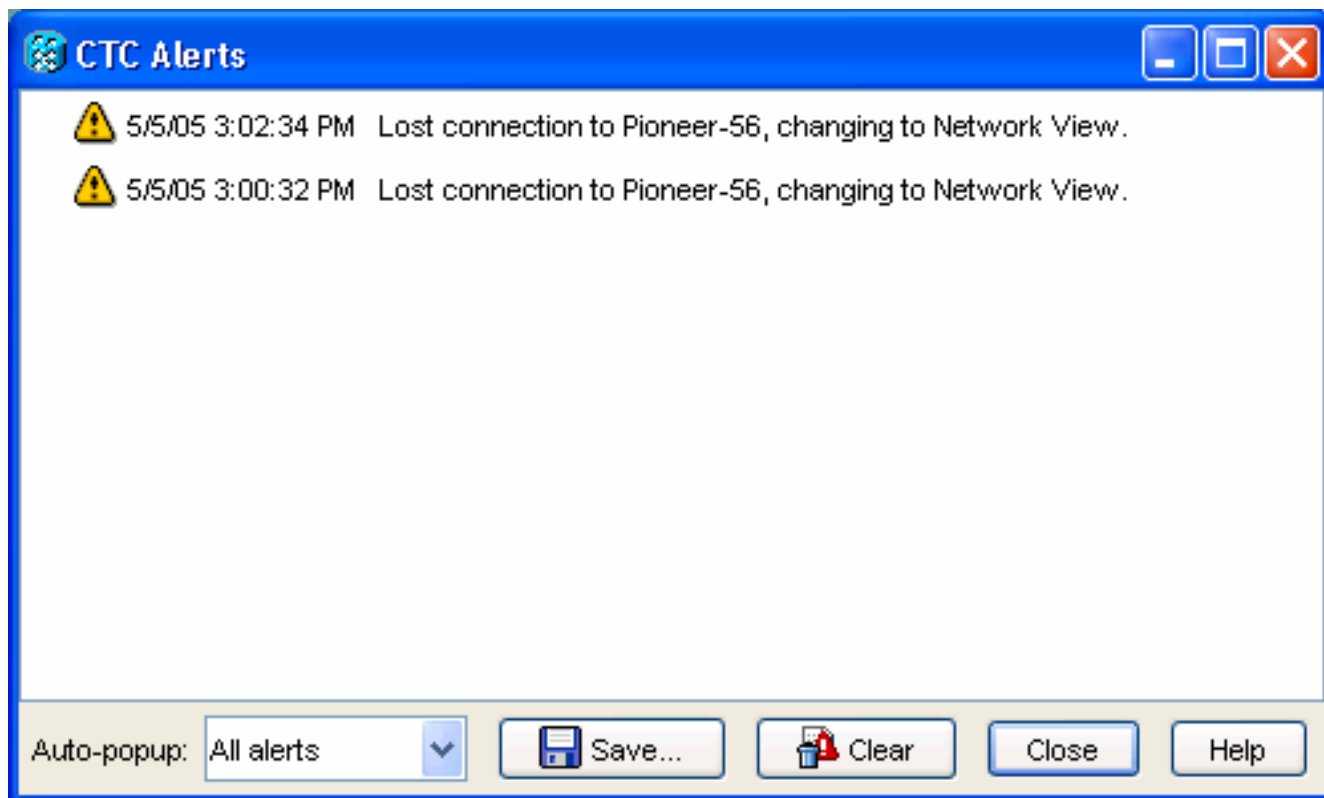
4. debug ip nat detailed コマンドを発行して、IP NAT 詳細トレースを有効にします。トレース ファイル内のアドレス変換を表示できます。たとえば、10.89.238.56 から 172.16.1.200 へのアドレス変換 ([図 5](#) の矢印 A を参照) および 172.16.1.200 から 10.89.238.56 へのアドレス変換が表示されます ([図 5](#) の矢印 B を参照)。 [図 5 - 詳述される Debug ip nat](#)

```
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55499]
NAT*: A 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] B
```

5. ルータで show access-list コマンドを発行し、アクセス リストを通過したパケットの数を表示します。 [図 6 - show access-list コマンド](#)

```
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)                                     アクセ
```

ス リストで TCC CORBA (IIOP) リスナー ポートがブロックされている場合、CTC と ONS 15454 のセッションが常にタイムアウトになり、次のような警告メッセージが 2 分おきに表示されます。 [図 7 - CTC アラート: TCC CORBA \(IIOP \) ポートのブロック](#)



この回避策は、CTC IIOP リスナー ポートを開けることです。Cisco Bug ID [CSCeh96275](#) ([登録ユーザ専用](#)) で、この問題が取り上げられています。将来的には、ファイアウォールで TCP ポート 80 および 1080 のコンジットを作成するだけで、ONS 15454 の実 IP アドレスの隠蔽がサポートされるようになります。

[トラブルシューティング](#)

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

[関連情報](#)

- [テクニカルサポートとドキュメント - Cisco Systems](#)