Utilice NAT para Ocultar la Dirección IP Real de ONS 15454 para Establecer una Sesión CTC

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para la traducción de direcciones de red (NAT) para establecer una sesión entre Cisco Transport Controller (CTC) y ONS 15454. La configuración utiliza NAT y una lista de acceso cuando el ONS 15454 reside en una red privada y el cliente CTC reside en una red pública.

Aplique NAT y una lista de acceso por motivos de seguridad. NAT oculta la dirección IP real de ONS 15454. La lista de acceso actúa como firewall para controlar el tráfico IP de entrada y salida del ONS 15454.

Prerequisites

Requirements

Antes de utilizar esta configuración, asegúrese de que cumple con los siguientes requisitos:

- Conozca de forma básica Cisco ONS 15454.
- Tenga en cuenta qué routers de Cisco admiten NAT.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS® Software Release 12.1(11) y posteriores
- Cisco ONS 15454 versión 5.X y posterior

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Esta sección proporciona la información básica esencial.

Topología

La topología de prueba incluye:

- Un Cisco ONS 15454, que actúa como servidor.
- Un PC, que actúa como cliente del Comité contra el Terrorismo.
- Un router de la serie 2600 de Cisco, que proporciona el soporte NAT.

Nota: Cisco ONS 15454 reside en la red interna y el PC está en la red externa.

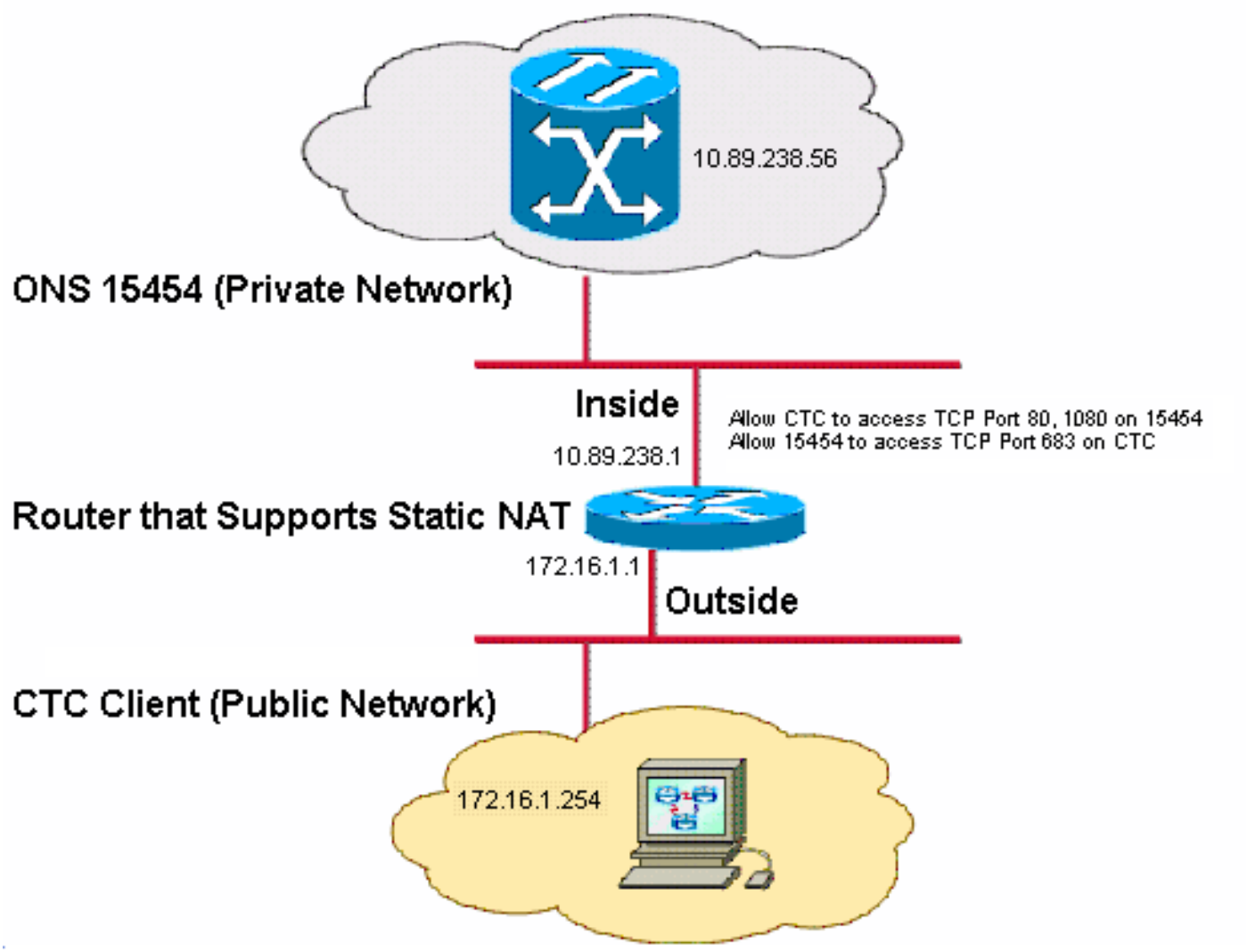
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Suponga que 172.16.0.0 es enrutable en la red pública.

Configuraciones

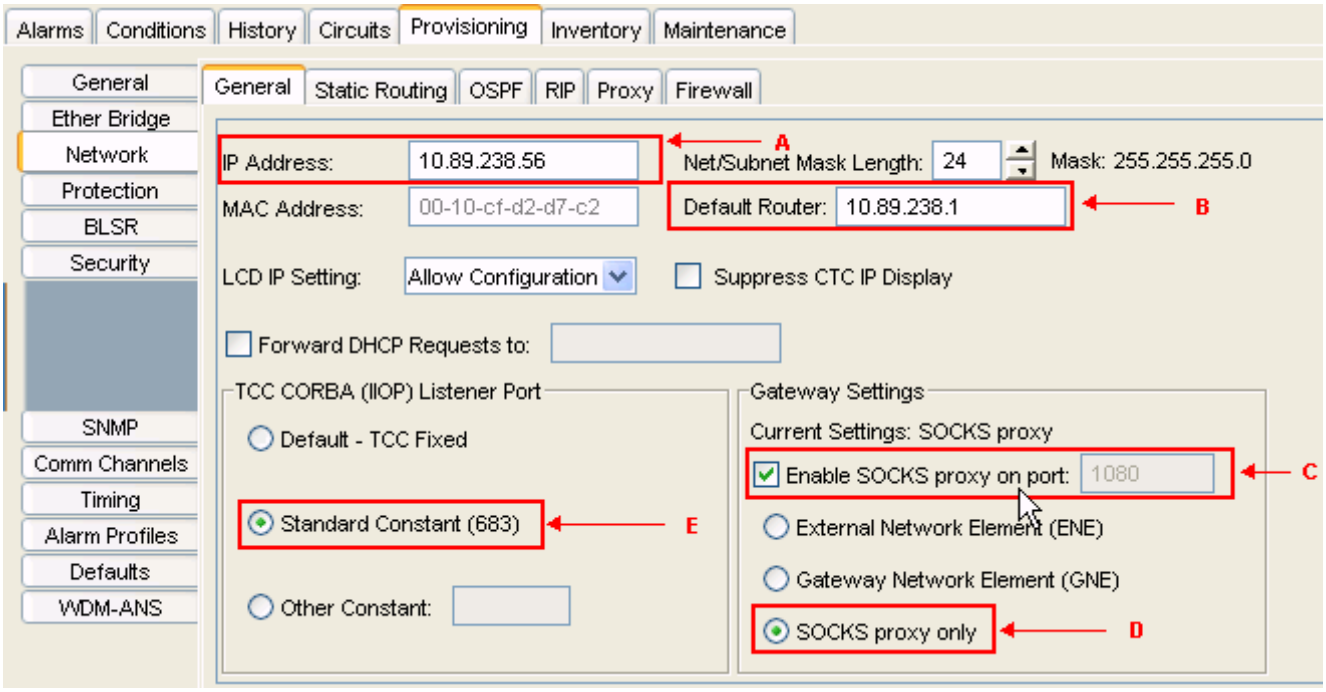
En este documento, se utilizan estas configuraciones:

- ONS 15454
- PC
- Router

Configuración de Cisco ONS 15454

Complete estos pasos:

1. En la vista de nodo, haga clic en **Provisioning > General > Network**.Verifique si la dirección IP del ONS 15454 aparece como 10.89.238.56 en el campo Dirección IP (consulte la flecha A en la Figura 2) y que el campo Router predeterminado contiene el valor 10.89.238.1 (consulte la flecha B en la Figura 2).**Figura 2: Configuración de ONS 15454**

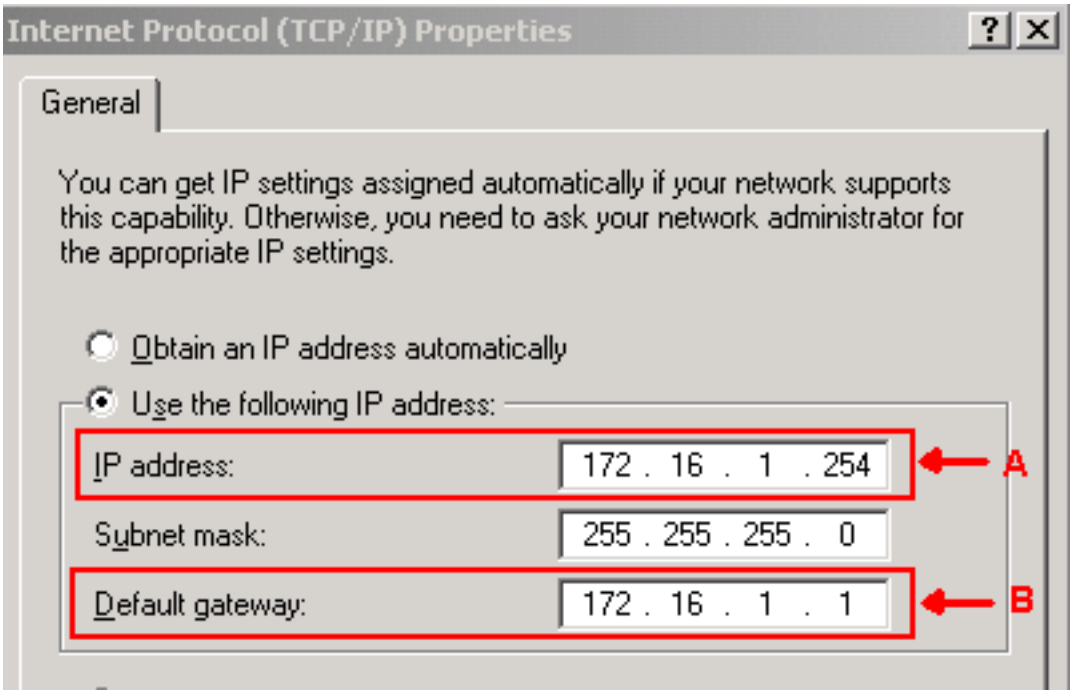


2. Marque la casilla de verificación **Enable SOCKS proxy on port** en la sección Gateway Settings (consulte la flecha C en la Figura 2) y seleccione la opción **SOCKS proxy only** (consulte la flecha D en la Figura 2).
3. Seleccione la opción de puerto del receptor necesaria en la sección Puerto del receptor TCC CORBA (IIOP). Dispone de estas tres opciones:**Predeterminado - TCC Fixed**: seleccione esta opción si el ONS 15454 se encuentra en el mismo lado del firewall que el equipo CTC, o si no hay firewall (predeterminado). Esta opción establece el puerto del receptor ONS 15454 en el puerto 57790. Puede utilizar la opción Default - TCC Fixed para acceder a través de un firewall si el puerto 57790 está abierto.**Constante estándar**: seleccione esta opción para utilizar el puerto 683, el número de puerto predeterminado de CORBA, como puerto del receptor ONS 15454. Este ejemplo utiliza la constante estándar (683) (consulte la flecha E en la figura 2).**Other Constant**: seleccione esta opción si no utiliza el puerto 683. Escriba el puerto IIOP que especifique el administrador del firewall.

Configuración del equipo personal

En el cuadro de diálogo Propiedades del protocolo de Internet (TCP/IP), verifique si el campo Dirección IP indica 172.16.1.254 como dirección IP de la PC (consulte la flecha A en la Figura 3). Compruebe también si 172.16.1.1 es el gateway predeterminado (consulte la flecha B en la Figura 3).

Figura 3: Configuración de PC



Configuración del router

Complete estos pasos:

1. Configure la interfaz interna donde reside Cisco ONS 15454.

```
!
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 la interfaz exterior donde reside el PC.

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

4. Configure la NAT estática.La configuración convierte la dirección IP 10.89.238.56 (local interno) en la dirección IP 172.16.1.200 (global externo). Ejecute el comando **show ip nat translation** en el router para ver la tabla de traducción (consulte la Figura 4).

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

Figura 4: Traducción NAT IP

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

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show access-list**: muestra el recuento de paquetes que pasan a través de la lista de acceso.

Procedimiento de verificación

Complete estos pasos para verificar la configuración:

1. Ejecute Microsoft Internet Explorer.
2. Escriba **http://172.16.1.200** en el campo Dirección de la ventana del explorador y presione ENTRAR.172.16.1.200 es la dirección global interna. En la red pública, los usuarios del CTC sólo pueden acceder a 172.16.1.200, que es la dirección global interna del ONS 15454 cuya dirección local interna es 10.89.238.56.Aparecerá la ventana Conexión CTC.
3. Escriba el nombre de usuario y la contraseña para iniciar sesión.El cliente CTC se conecta correctamente al ONS 15454.
4. Ejecute el comando **debug ip nat detail** para activar el seguimiento detallado de IP NAT. Puede ver las traducciones de direcciones en el archivo de seguimiento. Por ejemplo, la traducción de direcciones de 10.89.238.56 a 172.16.1.200 (consulte la flecha A en la Figura 5) y de 172.16.1.200 a 10.89.238.56 (consulte la flecha B en Figura 5).**Figura 5: Debug IP NAT Detallado**

```
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]
```

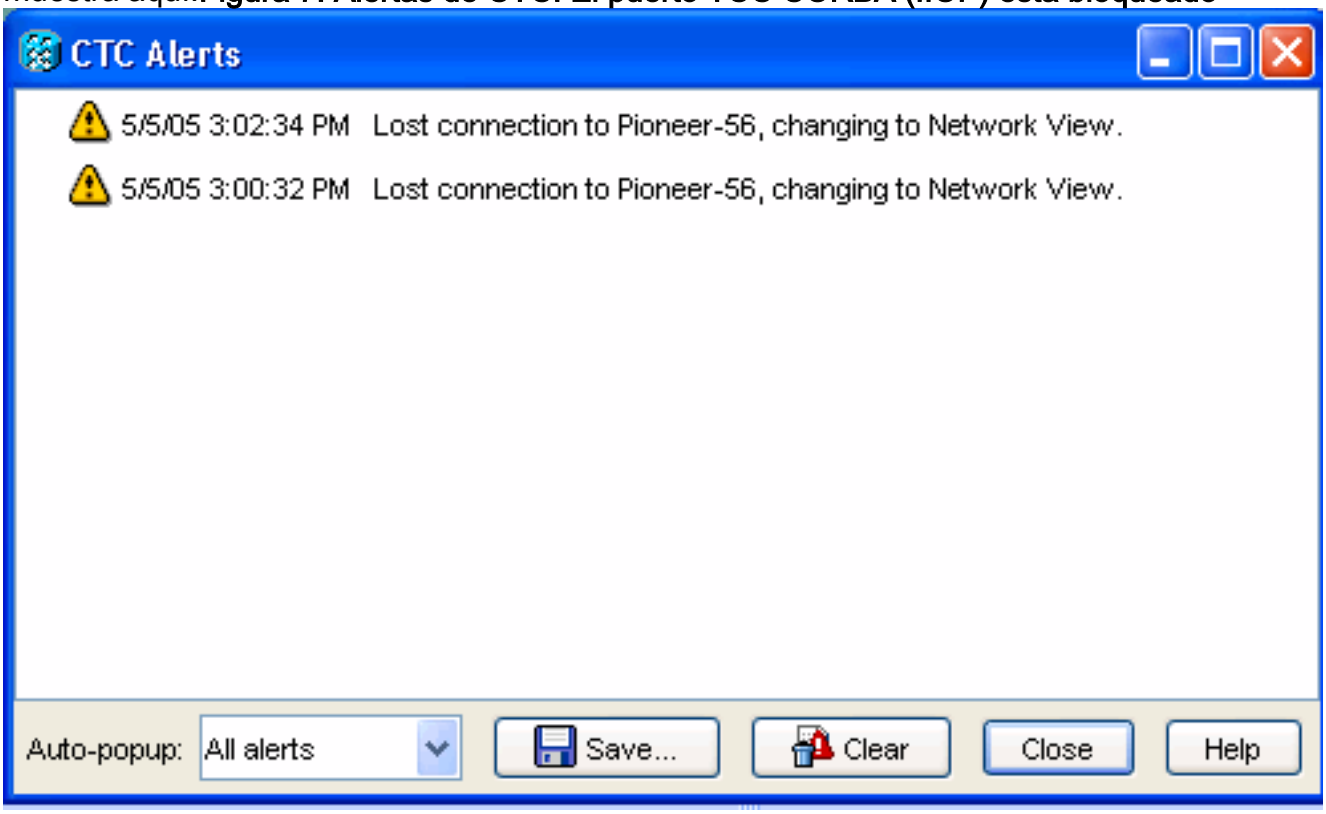
A → 10.89.238.56->172.16.1.200 ; B → 172.16.1.200->10.89.238.56

5. Ejecute el comando **show access-list** en el router para ver el conteo de paquetes que pasan a través de la lista de acceso.**Figura 6: Comando 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)
```

Si la lista de acceso bloquea el puerto del receptor TCC CORBA (IIOP), la sesión CTC con ONS

15454 se agota periódicamente y aparece un mensaje de alerta cada dos minutos como se muestra aquí:**Figura 7: Alertas de CTC: El puerto TCC CORBA (IIOP) está bloqueado**



Como solución alternativa, puede abrir el puerto del receptor CTC IIOP. El Id. de error de Cisco CSCeh96275 (sólo clientes registrados) aborda este problema.En el futuro, la creación de un conducto para los puertos TCP 80 y 1080 en el firewall es suficiente para proporcionar soporte para ocultar la dirección IP real de ONS 15454.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems