

# Utilice el NAT para ocultar el IP Address real del ONS15454 para establecer a una sesión CTC

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Topología](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del Cisco ONS 15454](#)

[Configuración de computadora personal](#)

[Configuración del router](#)

[Verificación](#)

[Procedimiento de verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## **Introducción**

Este documento proporciona una configuración de muestra para que el Network Address Translation (NAT) establezca una sesión entre el Cisco Transport Controller (CTC) y el ONS15454. La configuración utiliza el NAT y una lista de acceso cuando el ONS15454 reside en una red privada, y el cliente CTC reside en una red pública.

Aplique el NAT y una lista de acceso por motivos de seguridad. El NAT oculta el IP Address real del ONS15454. La lista de acceso sirve como Firewall controlar el tráfico IP dentro y fuera del ONS15454.

## **prerrequisitos**

### **Requisitos**

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

- Tenga conocimiento básico del Cisco ONS 15454.
- Sea consciente de los routers Cisco soportan el NAT.

## Componentes Utilizados

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

- Software Release 12.1(11) y Posterior de Cisco IOS®
- Versión 5.X y posterior del Cisco ONS 15454

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

## Antecedentes

Esta sección proporciona la información previa esencial.

## Topología

La Topología de prueba comprende:

- Un Cisco ONS 15454, que actúa como el servidor.
- Un PC, que sirve como el cliente CTC.
- Un Cisco 2600 Series Router, que proporciona el soporte NAT.

**Nota:** El 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 obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

## Diagrama de la red

En este documento, se utiliza esta configuración de red:

**Nota:** Asuma que 172.16.0.0 es routable en la red pública.

## Configuraciones

En este documento, se utilizan estas configuraciones:

- ONS15454
- PC
- Router

## Configuración del Cisco ONS 15454

Complete estos pasos:

1. En la vista de nodo, haga clic el **aprovisionamiento > el general > la red**. Verifique si la dirección IP del ONS15454 aparezca como 10.89.238.56 en el campo de la dirección IP (véase la flecha A en el [cuadro 2](#)), y que el campo del router predeterminado contiene el valor 10.89.238.1 (véase la flecha B en el [cuadro 2](#)). **Cuadro 2 – Configuración ONS15454**
2. Marque el **proxy de los CALCETINES del permiso en la** casilla de verificación del puerto en la sección de las configuraciones del gateway (véase el C de la flecha en el [cuadro 2](#)), y seleccione la opción del **proxy de los CALCETINES solamente** (véase la flecha D en el [cuadro 2](#)).
3. Seleccione la opción requerida del puerto del módulo de escucha en la sección de puerto del módulo de escucha TCC CORBA (IIOB). Usted tiene estas tres opciones: **Valor por defecto - TCC reparado** — Seleccione esta opción si el ONS15454 está en el mismo lado del Firewall como la computadora CTC, o si no hay Firewall (valor por defecto). Esta opción fija el puerto del módulo de escucha ONS15454 al puerto 57790. Usted puede utilizar el valor por defecto - El TCC reparó la opción para el acceso con un Firewall si el puerto 57790 está abierto. **Constante estándar** — Seleccione esta opción para utilizar el puerto 683, el número del puerto predeterminado CORBA, como el puerto del módulo de escucha ONS15454. Este ejemplo utiliza el constante estándar (683) (véase la flecha E en el [cuadro 2](#)). **El otro constante** — Seleccione esta opción si usted no utiliza el puerto 683. Teclee el puerto IIOB que su administrador de firewall especifica.

## Configuración de computadora personal

En el cuadro de diálogo Propiedades del protocolo de Internet (TCP/IP), verifique si el campo de la dirección IP indique 172.16.1.254 como la dirección IP del PC (véase la flecha A en el [cuadro 3](#)). También marque si 172.16.1.1 es el default gateway (véase la flecha B en el [cuadro 3](#)).

### Cuadro 3 – Configuración de la PC

#### Configuración del router

Complete estos pasos:

1. Configure la interfaz interior donde reside el 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 el 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 el NAT estático. La configuración convierte la dirección IP de 10.89.238.56 (Inside Local) a la dirección IP de 172.16.1.200 (Outside Global). Publique el **comando show ip nat translation** en el router de ver la tabla de traducción (véase el [cuadro 4](#)).!

```

ip nat inside source static 10.89.238.56 172.16.1.200
!

```

! **Cuadro 4 – Traducción de NAT IP**

## 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.

- **lista de acceso de la demostración** — visualiza la cuenta de los 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. Teclee **http://172.16.1.200** en el campo de dirección de la ventana del buscador, y el Presione ENTER. 172.16.1.200 es la dirección global interna. En la red pública, los usuarios CTC pueden acceder solamente 172.16.1.200, que es la dirección global interna del ONS15454 cuya dirección local interna es 10.89.238.56. La ventana CTC login (Registro de CTC) aparece.
3. Teclee el Nombre de usuario y la contraseña para iniciar sesión. El cliente CTC conecta con éxito con el ONS15454.
4. Publique el **comando debug ip nat detailed** de girar la traza detallada NAT IP. Usted puede ver las traducciones de la dirección en el archivo de traza. Por ejemplo, traducción de la dirección de 10.89.238.56 a 172.16.1.200 (véase la flecha A en el [cuadro 5](#)), y de 172.16.1.200 a 10.89.238.56 (véase la flecha B en el [cuadro 5](#)). **Cuadro 5 – IP NAT del debug detallado**
5. **Comando show access-list** del problema en el router de ver la cuenta de los paquetes que pasan a través de la lista de acceso. **Cuadro 6 – El comando show access-list** Si la lista de acceso bloquea el puerto del módulo de escucha TCC CORBA (IIOP), la sesión CTC con los tiempos ONS15454 hacia fuera regularmente, y un mensaje de alerta aparece cada dos minutos como se muestra aquí: **Cuadro 7 – Alertas CTC: Se bloquea el puerto TCC CORBA**

(IIOP) Como solución alternativa, usted puede abrir el puerto del módulo de escucha CTC IIOP. El Id. de bug Cisco [CSCeh96275](#) ([clientes registrados solamente](#)) aborda este problema. En el futuro, la creación de un conducto para el puerto TCP 80 y 1080 en el Firewall es bastante para proporcionar el soporte para ocultar el IP Address real del ONS15454.

## [Troubleshooting](#)

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

## [Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)