# 使用NAT隐藏ONS15454实际IP地址建立CTC会

```
目录
```

简介 先决条件 要求 使用的组件 规则 背景信息 拓扑 配置 网络图 配置 思科ONS 15454配置 个人计算机配置 路由器配置 验证 验证过程 故障排除 相关信息

# <u>简介</u>

本文档提供了网络地址转换(NAT)的示例配置,用于在思科传输控制器(CTC)和ONS 15454之间建 立会话。当ONS 15454驻留在专用网络中且CTC客户端驻留在公共网络中时,该配置使用NAT和访 问列表。

为安全起见应用NAT和访问列表。NAT隐藏了ONS 15454的实际IP地址。访问列表用作防火墙来控 制进出ONS 15454的IP流量。

# <u>先决条件</u>

## <u>要求</u>

尝试进行此配置之前,请确保满足以下要求:

- •了解Cisco ONS 15454的基本知识。
- •了解哪些Cisco路由器支持NAT。

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- •思科IOS®软件版本12.1(11)及更高版本
- Cisco ONS 15454 5.X版及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

#### <u>规则</u>

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

## <u>背景信息</u>

本节提供基本背景信息。

#### <u>拓扑</u>

测试拓扑包括:

- 一个Cisco ONS 15454,用作服务器。
- 一台用作CTC客户端的PC。
- •一台Cisco 2600系列路由器,提供NAT支持。

注意:Cisco ONS 15454位于内部网络中,PC位于外部网络中。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注:要**查找有关本文档中使用的命令的其他信息,请使用命<u>令查找工</u>具(<u>仅注</u>册客户)。

#### <u>网络图</u>

本文档使用以下网络设置:



注意:假设172.16.0.0在公共网络中可路由。

#### <u>配置</u>

本文档使用以下配置:

- ONS 15454
- PC
- 路由器

#### <u>思科ONS 15454配置</u>

请完成以下步骤:

 在节点视图中,单击Provisioning > General > Network。验证ONS 15454的IP地址是否显示为 10.89.238.56(在图2中参见箭头A),以及"默认路由器"字段是否包含值10.89.238.1(参见图 2中的箭头B)。图2 - ONS 15454配置

Alarms Conditions	History Circuits	Provisioning Inventory	Maintenance			
General	General Static Routing OSPF RIP Proxy Firewall					
Ether Bridge						
Network	IP Address:	10.89.238.56	Net/Subnet Mask Length: 24 🚔 Mask: 255.255.255.0			
Protection	MAC Addresse:	00.10 of d2 d7 c2	Defeut Router: 10.89.238.1			
BLSR	WAC Address.	00-10-01-02-07-02	Derault Nouler. 10.03.200.1			
Security	LCD IP Setting:	Allow Configuration 🔽	Suppress CTC IP Display			
	Forward DHCP Requests to:     Gateway Settings					
SNMP	O Default - TCC Fixed		Current Settings: SOCKS proxy			
Comm Channels			Enable SOCKS proxy on port: 1080			
Timing						
Alarm Profiles	Standard Constant (683) E C External Network Element (ENE)					
Defaults WDM-ANS	◯ Other Consta	ant:	<ul> <li>◯ Gateway Network Element (GNE)</li> <li>☑ SOCKS proxy only</li> </ul>			

- 2. 选中"**网关设置"部分的"启用端口上的SOCKS代理"**复选框(请参阅图2中的箭头C)<u>,并选择仅</u> <u>SOCKS代理</u>选项(请参阅图2中的箭头D)。
- 3. 在"TCC CORBA(IIOP)侦听器端口"部分中,选择所需的侦听器端口选项。您有以下三个选项 : Default - TCC Fixed — 如果ONS 15454与CTC计算机位于防火墙的同一侧,或者没有防火 墙(默认),请选择此选项。此选项将ONS 15454侦听器端口设置为端口57790。如果端口 57790打开,则可以使用Default - TCC Fixed选项通过防火墙访问。标准常量 — 选择此选项以 使用端口683(CORBA默认端口号)作为ONS 15454侦听器端口。此示例使用标准常量 (683)(请参阅图2中的箭头E)。其他常量 — 如果不使用端口683,请选择此选项。键入防火墙 管理员指定的IIOP端口。

## <u>个人计算机配置</u>

在"Internet协议(TCP/IP)属性"对话框中,验证IP地址字段是否将172.16.1.254表示为PC的IP地址(请参阅图3中的箭<u>头A</u>)。 另请检查172.16.1.1是否是默认网关(请参阅图3中的<u>箭头B</u>)。

#### 图3 - PC配置

nternet Protocol (TCP/IP) Propertie	es <u>?X</u>				
General					
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.					
O <u>O</u> btain an IP address automatically					
• Use the following IP address:					
<u>I</u> P address:	172 . 16 . 1 . 254 🗕 🗕 A				
S <u>u</u> bnet mask:	255 . 255 . 255 . 0				
Default gateway:	172.16.1.1 <b>—</b> B				

#### <u>路由器配置</u>

请完成以下步骤:

1 interface Ethernet1/0 ip address 10.89.238.1 255.255.255.0 ip access-group 101 in ip nat inside 1 2. 配置访问列表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 1 access-list 101 permit tcp any any eq 683 ! ! Allow ONS 15454 to access TCP Port 683 on the PC Т 3. 配置PC所在的外部接口。

interface Ethernet1/1
ip address 172.16.1.1 255.255.255.0
ip nat outside
'

1. 配置Cisco ONS 15454所在的内部接口。

4. 配置静态 NAT。配置将IP地址10.89.238.56(内部本地)转换为IP地址172.16.1.200(外部全局)。在路由器上发出show ip nat translation命令,查看转换表(请参见图4)。

ip nat inside source static 10.89.238.56 172.16.1.200

图4 - IP NAT转换

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

## <u>验证</u>

Т

本部分所提供的信息可用于确认您的配置是否正常工作。

<u>命令输出解释程序工具(仅限注册用户)支持某些</u> show <mark>命令,使用此工具可以查看</mark>对 show 命令 输出的分析。

• show access-list — 显示通过访问列表的数据包计数。

#### 验证过程

完成以下步骤以验证配置:

- 1. 运行Microsoft Internet Explorer。
- 2. 在浏览器窗口的Address字段中键入http://172.16.1.200,然后按ENTER键。172.16.1.200是内

部全局地址。在公共网络中,CTC用户只能访问172.16.1.200,即ONS 15454的内部全局地址 ,其内部本地地址为10.89.238.56。系统将显示CTC Login(CTC登录)窗口。

- 3. 键入要登录的用户名和密码。CTC客户端成功连接到ONS 15454。
- 4. 发出debug ip nat detailed命令以打开IP NAT详细跟踪。您可以在跟踪文件中查看地址转换。 例如,从10.89.238.56到172.16.1.200的地址转换(请参阅图5中的箭头A)和从 172.16.1.200到10.89.238.56的地址转换(请参阅箭头A)b在图<u>5中</u>)。图5 — 调试IP NAT详细 信息

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\*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [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\*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32895] NAT\*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [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] NAT\*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32897] NAT\*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32897] S. 在路由器上发出show access-list命令, 查看通过访问列表的数据包计数。图6-show access-list命令 2600-4#show access-list 101 permit tcp any eq uww any (56 matches) permit tcp any eq 1080 any (330 matches) permit tcp any eq 683 (6 matches)  $\mu$ Rio DID=BULTCC COPRALION/60058880 INFERENCE (15000-4480050-4

问列表阻止TCC CORBA(IIOP)侦听器端口,则与ONS 15454的CTC会话会定期超时,并且每 两分钟显示一条警报消息,如下所示:**图7 - CTC警报:TCC CORBA(IIOP)端口被阻止** 

😫 CTC Alerts				
\Lambda 5/5/05 3:02:34 PM	Lost connection to Pioneer-56, changing to Network View.			
📤 5/5/05 3:00:32 PM	/5/05 3:00:32 PM   Lost connection to Pioneer-56, changing to Network View.			
Auto-popup: All alerts	V 🕞 Save 🍄 Clear Close	Help		

解决方法是,您可以打开CTC IIOP侦听器端口。Cisco Bug ID <u>CSCeh96275(仅注</u>册客户)可解 决此问题。将来,在防火墙上为TCP端口80和1080创建管道足以提供隐藏ONS 15454实际 IP地址的支持。

# <u>故障排除</u>

目前没有针对此配置的故障排除信息。

# 相关信息

• <u>技术支持和文档 - Cisco Systems</u>