Utiliser NAT pour masquer l'adresse IP réelle d'ONS 15454 pour établir une session CTC

Contenu

Introduction

Ce document fournit un exemple de configuration pour la traduction d'adresses de réseau (NAT) pour établir une session entre Cisco Transport Controller (CTC) et ONS 15454. La configuration utilise NAT et une liste d'accès lorsque l'ONS 15454 réside dans un réseau privé et que le client CTC réside dans un réseau public.

Appliquer la NAT et une liste d'accès à des fins de sécurité. NAT masque l'adresse IP réelle de ONS 15454. La liste d’accès sert de pare-feu pour contrôler le trafic IP entrant et sortant de l’ONS 15454.

Conditions préalables

Conditions requises

Assurez-vous de répondre à ces exigences avant d'essayer cette configuration :

- Connaître de base Cisco ONS 15454.
- Sachez quels routeurs Cisco prennent en charge la fonction NAT.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS® Version 12.1(11) et ultérieure
- Cisco ONS 15454 version 5.X et ultérieure

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Cette section fournit les informations de base essentielles.

Topologie

La topologie de test comprend :

- Un Cisco ONS 15454, qui fait office de serveur.
- Un PC, qui sert de client CTC.
- Un routeur de la gamme Cisco 2600 qui prend en charge la fonction NAT.

Remarque : Cisco ONS 15454 réside dans le réseau interne et le PC dans le réseau externe.

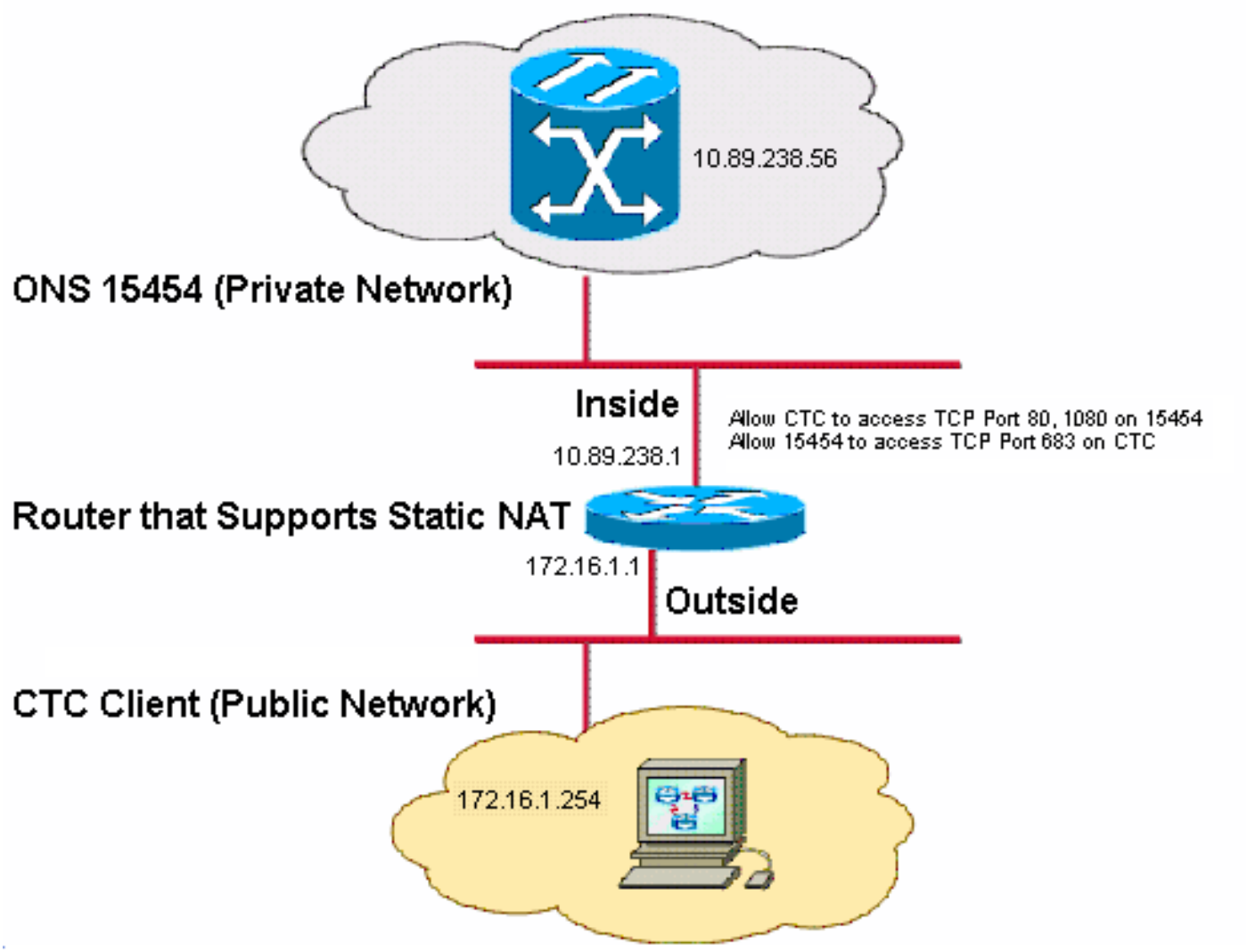
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque : Supposez que 172.16.0.0 est routable dans le réseau public.

Configurations

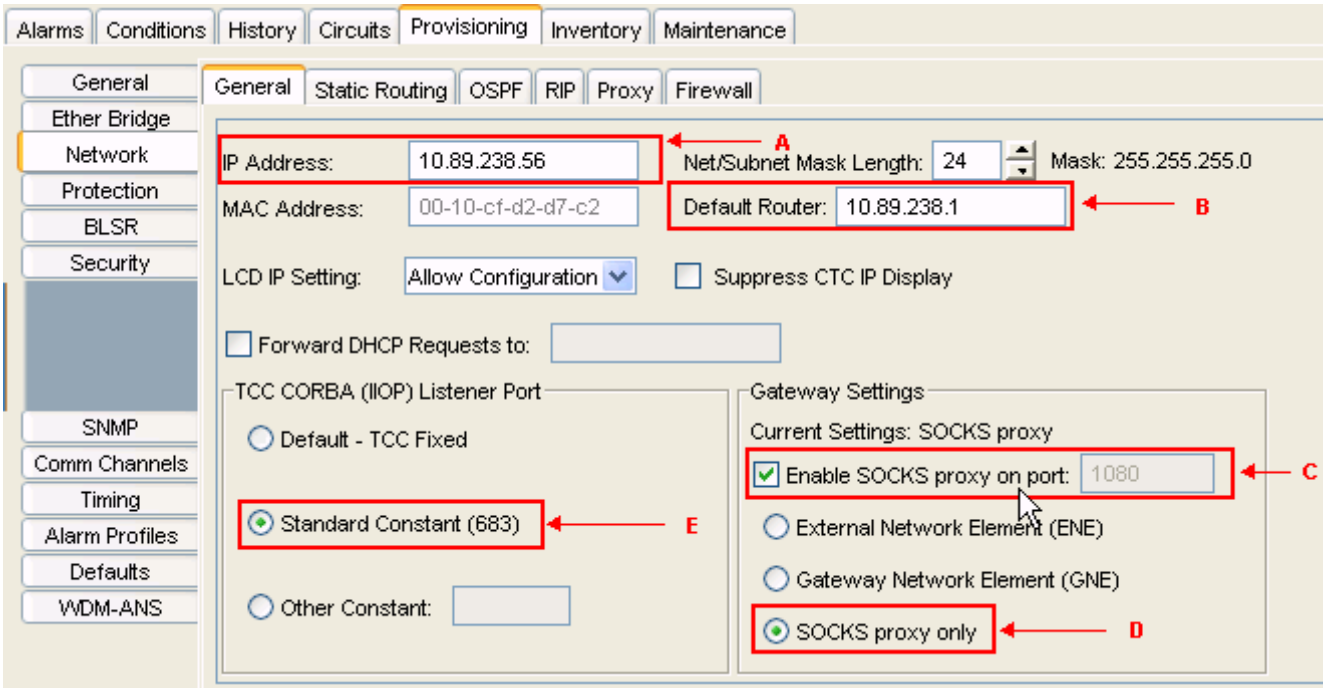
Ce document utilise les configurations suivantes :

- ONS 15454
- PC
- Routeur

Configuration de Cisco ONS 15454

Procédez comme suit :

1. Dans la vue noeud, cliquez sur **Provisioning > General > Network**.Vérifiez si l'adresse IP de l'ONS 15454 apparaît sous la forme 10.89.238.56 dans le champ IP Address (voir la flèche A à la figure 2) et si le champ Default Router contient la valeur 10.89.238.1 (voir la flèche B à la figure 2).**Figure 2 : configuration ONS 15454**

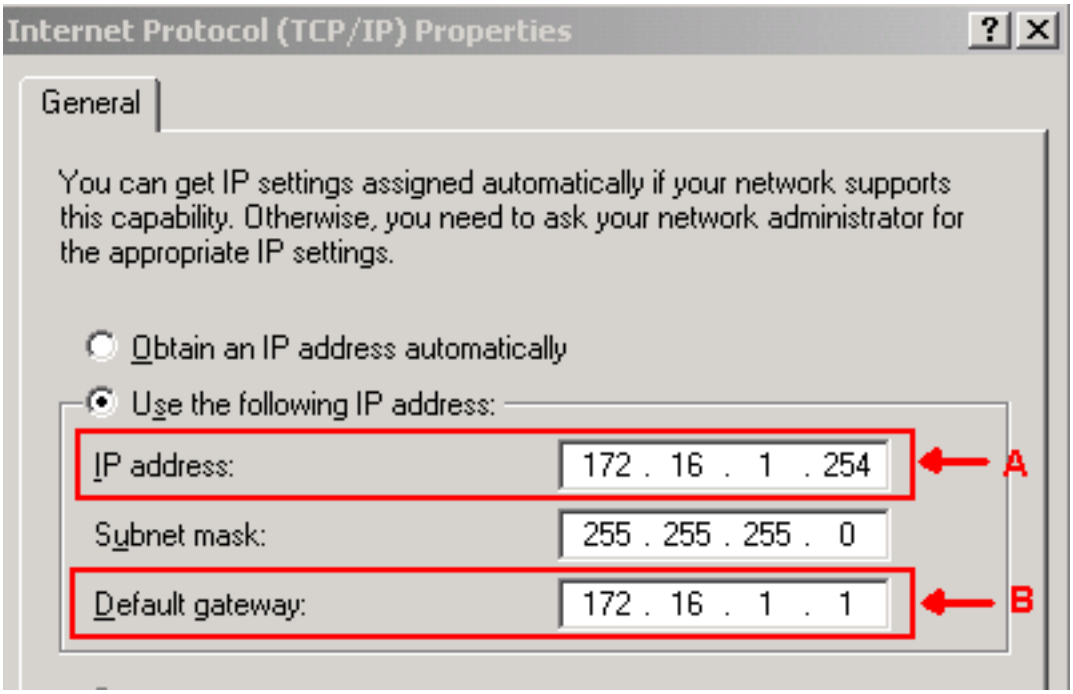


2. Cochez la case **Activer le proxy SOCKS sur le port** dans la section Paramètres de la passerelle (voir la flèche C dans la Figure 2) et sélectionnez l'option **proxy SOCKS uniquement** (voir la flèche D dans la Figure 2).
3. Sélectionnez l'option de port d'écouteur requise dans la section TCC CORBA (IOP) Listener Port. Vous disposez des trois options suivantes :**Default - TCC Fixed** : sélectionnez cette option si l'ONS 15454 se trouve du même côté du pare-feu que l'ordinateur CTC ou s'il n'y a pas de pare-feu (par défaut). Cette option définit le port d'écoute ONS 15454 sur le port 57790. Vous pouvez utiliser l'option Par défaut - TCC Fixe pour l'accès via un pare-feu si le port 57790 est ouvert.**Standard Constant** : sélectionnez cette option pour utiliser le port 683, le numéro de port par défaut CORBA, comme port d'écoute ONS 15454. Cet exemple utilise la constante standard (683) (voir la flèche E à la Figure 2).**Autre constante** : sélectionnez cette option si vous n'utilisez pas le port 683. Tapez le port IIOP spécifié par votre administrateur de pare-feu.

Configuration de l'ordinateur personnel

Dans la boîte de dialogue Propriétés du protocole Internet (TCP/IP), vérifiez si le champ Adresse IP indique 172.16.1.254 comme adresse IP du PC (voir la flèche A à la Figure 3). Vérifiez également si 172.16.1.1 est la passerelle par défaut (voir la flèche B à la Figure 3).

Figure 3 - Configuration du PC



Configuration du routeur

Procédez comme suit :

1. Configurez l'interface interne où réside 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. Configurez la liste d'accès 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. Configurez l'interface externe sur laquelle réside le PC.
```
interface Ethernet1/1
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
!
```
4. Configurez la NAT statique.La configuration convertit l'adresse IP 10.89.238.56 (locale interne) en adresse IP 172.16.1.200 (globale externe). Exécutez la commande **show ip nat translation** sur le routeur pour afficher la table de traduction (voir Figure 4).
```
!
ip nat inside source static 10.89.238.56 172.16.1.200
!
```
Figure 4 : Traduction 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  ---            ---
```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show access-list** - affiche le nombre de paquets qui traversent la liste d'accès.

Procédure de vérification

Effectuez les étapes suivantes pour vérifier la configuration :

1. Exécutez Microsoft Internet Explorer.
2. Tapez **http://172.16.1.200** dans le champ Adresse de la fenêtre du navigateur, puis appuyez sur ENTRÉE.172.16.1.200 est l'adresse globale interne. Dans le réseau public, les utilisateurs CTC ne peuvent accéder qu'à 172.16.1.200, qui est l'adresse globale interne de l'ONS 15454 dont l'adresse locale interne est 10.89.238.56.La fenêtre Connexion CCT s'affiche.
3. Tapez le nom d'utilisateur et le mot de passe pour vous connecter.Le client CTC se connecte correctement à l'ONS 15454.
4. Exécutez la commande **debug ip nat detail** pour activer la trace détaillée NAT IP. Vous pouvez afficher les traductions d'adresses dans le fichier de suivi. Par exemple, la traduction d'adresses de 10.89.238.56 à 172.16.1.200 (voir la flèche A dans la figure 5) et de 172.16.1.200 à 10.89.238.56 (voir la flèche B dans Figure 5).**Figure 5 - Détail du débogage de la NAT IP**

```
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]
```

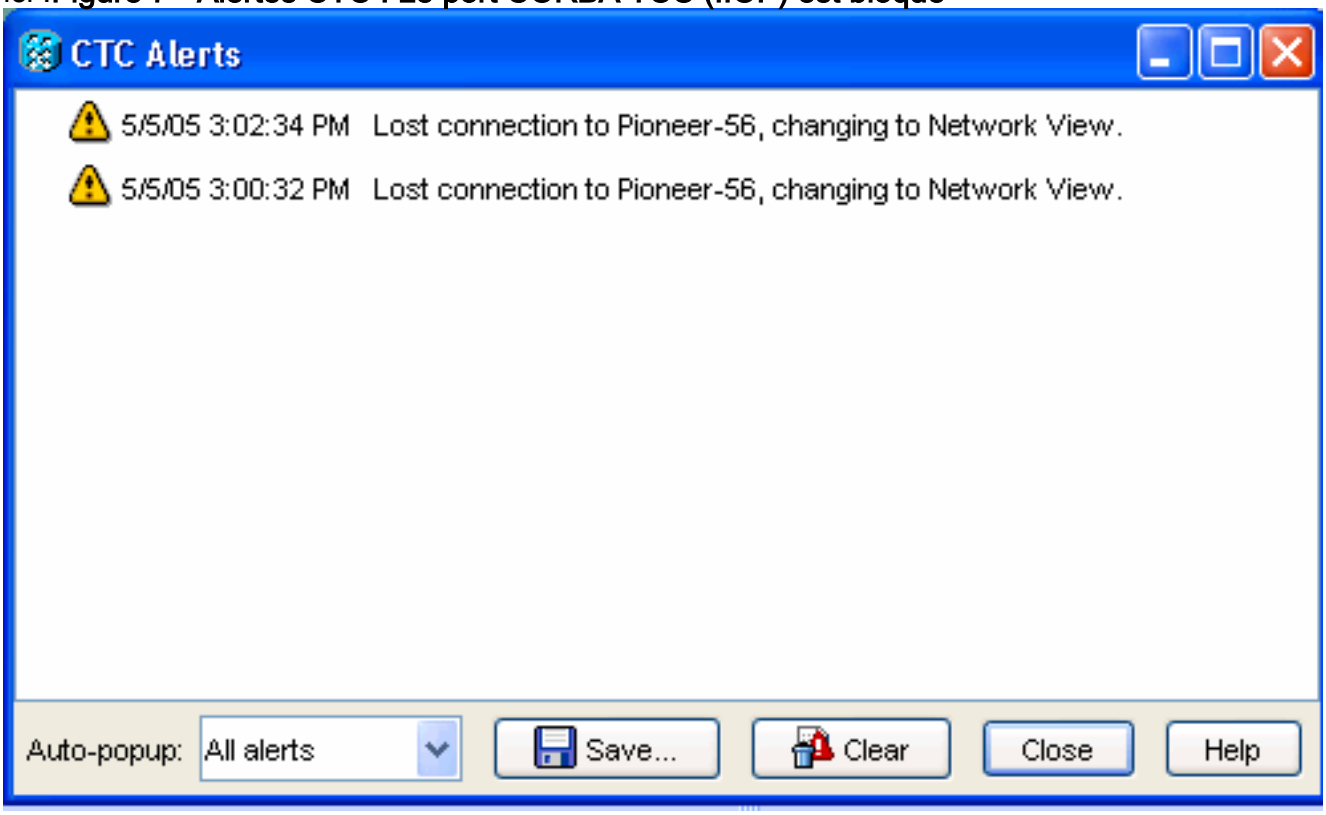
A → 10.89.238.56->172.16.1.200 ; B → 172.16.1.200->10.89.238.56

5. Exécutez la commande **show access-list** sur le routeur pour afficher le nombre de paquets qui traversent la liste d'accès.**Figure 6 - Commande 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

liste d'accès bloque le port d'écoute TCC CORBA (IIOP), la session CTC avec ONS 15454 expire régulièrement et un message d'alerte s'affiche toutes les deux minutes comme indiqué ici :**Figure 7 - Alertes CTC : Le port CORBA TCC (IIOP) est bloqué**



Comme solution de contournement, vous pouvez ouvrir le port d'écoute IIOP CTC. L'ID de bogue Cisco CSCeh96275 (clients enregistrés uniquement) répond à ce problème.À l'avenir, la création d'un conduit pour les ports TCP 80 et 1080 sur le pare-feu suffit à fournir la prise en charge pour masquer l'adresse IP réelle de ONS 15454.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems