

# H3C MSRルーターのアウトバウンド双方向 NATの設定例(Comware V7)

Copyright©2014 H3C Technologies Co.,Ltd. All rights reserved.

本マニュアルのいかなる部分も、杭州H3C Technologies Co.,Ltd. の書面による  
事前の同意がない限り、いかなる形式または手段によっても複製または送信するこ  
とはできません。本マニュアルの情報は、予告なしに変更されることがあります。

The H3C logo is displayed in a bold, red, sans-serif font. The letters 'H', '3', and 'C' are connected, with the '3' being slightly smaller and positioned between the 'H' and 'C'.

# 内容

はじめに.....	3
前提条件.....	3
例:アウトバウンド双方向NATの設定.....	3
ネットワーク要件.....	3
要件分析.....	4
使用しているソフトウェアのバージョン.....	4
設定手順.....	4
設定の確認.....	5
設定ファイル.....	7
関連ドキュメント.....	8

# はじめに

このドキュメントでは、アウトバウンド双方向NATの設定例について説明します。

## 前提条件

この文書は、Comware V 7ベースのMSRルーターに適用されます。例の手順と情報は、ルーターのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

このドキュメントの設定例は、ラボ環境で作成および検証されたものであり、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、すべてのコマンドがネットワークに与える潜在的な影響を理解していることを確認してください。

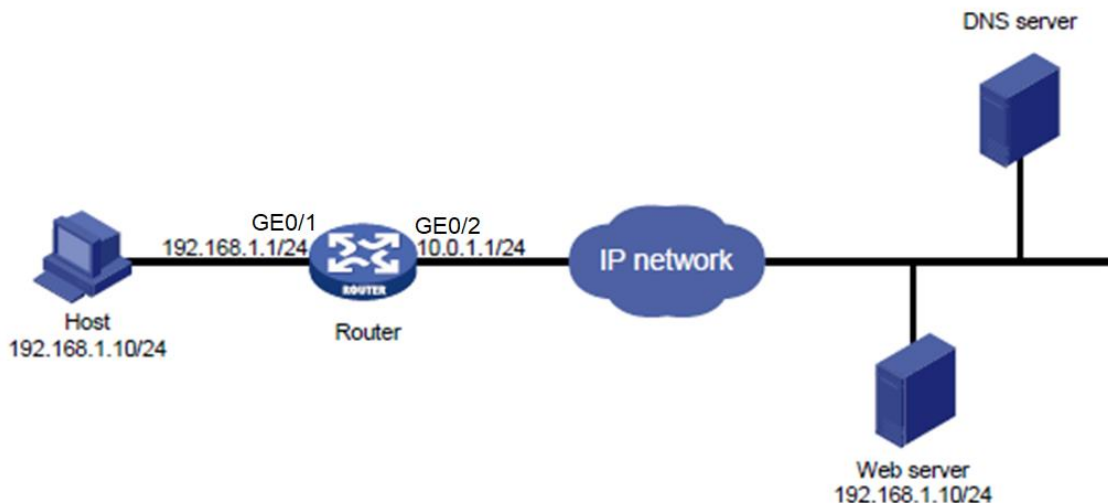
このマニュアルでは、NATに関する基本的な知識があることを前提としています。

## 例:アウトバウンド双方向NATの設定

### ネットワーク要件

図1に示すように、ルーターは企業のプライベートネットワークのゲートウェイとして機能します。プライベートネットワークは、Webサーバーが存在するサブネットと重複します。企業には、2つのパブリックIPアドレス202.38.1.2と202.38.1.3があります。サーバーのドメイン名を使用して、内部ホストが外部WebサーバーにアクセスできるようにNATを構成します。

図1 ネットワークダイアグラム



# 要件分析

ネットワーク要件を満たすには、次のタスクを実行する必要があります。

- ALGを使用したインバウンドダイナミックNATを設定して、内部ホストが別の内部ホストではなくWebサーバーに到達するようにします。プライベートネットワークは、次のサブネットと重複しません。  
Webサーバーが存在します。ALGを使用するNATは、DNS応答ペイロード内のWebサーバーのIPアドレスを、動的に割り当てられたパブリックアドレスに変換できます。
- 内部ホストからのパケットの送信元IPアドレスをダイナミックに割り当てられたパブリックアドレスに変換するように、アウトバウンドダイナミックNATを設定します。
- スタティックルートを外部WebサーバーのパブリックIPアドレスに追加します。

補足:FTP, TFTP, SIP, DNSなどのプロトコルでは宛先のIPアドレスが、TCPヘッダーではなく、それぞれのプロトコルヘッダーに含まれていて、NATのアドレス変換がプロトコルヘッダー部分のみなので、正しい通信が行われません。従って、プロトコルを意識したプロトコルヘッダーのアドレス変換を行うのがALG(Application Layer Gateway)です。

## 使用しているソフトウェアのバージョン

この設定例は、R0106で作成および検証されています。

## 設定手順

#ルーターのインターフェイスにIPアドレスを割り当てます。

```
<Router> system-view
```

```
[Router] interface gigabitethernet 0/1
```

```
[Router-GigabitEthernet0/1] ip address 192.168.1.1 24
```

```
[Router-GigabitEthernet0/1] quit
```

```
[Router] interface gigabitethernet 0/2
```

```
[Router-GigabitEthernet0/2] ip address 10.0.1.1 24
```

```
[Router-GigabitEthernet0/2] quit
```

#DNS用にALGを使用したNATを有効にします。

```
[Router] nat alg dns
```

#サブネット192.168.1.0/24からのパケットがNATされることを許可するようにACL 2000を設定します。

```
[Router] acl number 2000
```

```
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
```

```
[Router-acl-basic-2000] quit
```

#アドレスグループ1を作成します。

```
[Router] nat address-group 1
```

#グループにパブリックIPアドレス202.38.1.2を追加します。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
```

```

[Router-nat-address-group-1] quit
#アドレスグループ2を作成します。
[Router] nat address-group 2
#グループにパブリックIPアドレス202.38.1.3を追加します。
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit

#GigabitEthernet 0/2でインバウンドNO-PATをイネーブルにして、DNS応答ペイロード内のWebサーバーのIPアドレスをアドレスグループ1のIPアドレスに変換します。リバーシブルNATを許可します。
[Router] interface gigabitethernet 0/2
[Router-GigabitEthernet0/2] nat inbound 2000 address-group 1 no-pat reversible

#GigabitEthernet 0/2で発信PATをイネーブルにして、発信パケットの送信元IPアドレスをアドレスグループ2のパブリックIPアドレスに変換します。
[Router-GigabitEthernet0/2] nat outbound 2000 address-group 2
[Router-GigabitEthernet0/2] quit

#出インターフェイスとしてGigabitEthernet 0/2を使用し、202.38.1.2へのスタティックルートを設定します。
ネクストホップとして10.0.1.1。
[Router] ip route-static 202.38.1.2 32 gigabitethernet 0/2 10.0.1.1

```

## 設定の確認

#内部ホストが、サーバーのドメイン名を使用してWebサーバーにアクセスできることを確認します (詳細は省略)。

#すべてのNAT設定を表示し、NATが正しく設定され、ALGを使用するNATがイネーブルになっていることを確認します。

```
[Router] display nat all
```

NAT address group information:

There are 2 NAT address groups.

Address group 1:

Address information:

Start address	End address
202.28.1.2	202.38.1.2

Address group 2:

Address information:

Start address	End address
202.28.1.3	202.38.1.3

NAT inbound information:

There are 1 NAT inbound rules.

Interface: GigabitEthernet1/2

ACL: 2000	Address group: 1	Add route: N
NO-PAT: Y	Reversible: Y	5

NAT outbound information:

There are 1 NAT outbound rules.

Interface: GigabitEthernet1/2

ACL: 2000            Address group: 2            Port-preserved:  
N NO-PAT: N        Reversible: N

NAT logging:

Log enable            : Disabled  
Flow-begin            : Disabled  
Flow-end              : Disabled  
Flow-active         : Disabled Port-  
block-assign         : Disabled Port-  
block-withdraw       : Disabled  
Alarm                 :  
Disabled

NAT mapping behavior:

Mapping mode: Address and Port-  
Dependent ACL :---

NAT ALG:

DNS            :Enabled  
FTP            : Enabled  
H323         : Enabled  
ICMP-ERROR    :  
Enabled ILS    :  
Enabled  
MGCP          : Enabled  
NBT           : Enabled  
PPTP          : Enabled  
RSH           : Enabled  
RTSP          : Enabled  
SCCP          : Enabled  
SIP           : Enabled  
SQLNET        : Enabled  
TFTP          : Enabled  
XDMCP         : Enabled

#NATセッションを表示し、ホストがNATを介してWebサーバーにアクセスできることを確認します。

[Router] display nat session verbose Initiator:

Source        IP/port: 192.168.1.10/1694  
Destination IP/port: 202.38.1.2/8080  
VPN instance/VLAN ID/VLL ID: -/-/

Protocol: TCP(6)  
Responder:  
Source IP/port: 192.168.1.10/8080  
Destination IP/port: 202.38.1.3/1025  
VPN instance/VLAN ID/VLL ID: -/-/  
Protocol: TCP(6)  
State: TCP\_ESTABLISHED  
Application: HTTP  
Start time: 2013-08-15 14:53:29 TTL: 3597s  
Interface(in) : GigabitEthernet1/1 Interface(out):  
GigabitEthernet1/2  
Initiator->Responder: 7 packets 308 bytes  
Responder->Initiator: 5 packets 312 bytes  
  
Total sessions found: 1

## 設定ファイル

```
#  
interface GigabitEthernet0/1  
    port link-mode route  
    ip address 192.168.1.1 255.255.255.0  
#  
interface GigabitEthernet0/2  
    port link-mode route  
    ip address 10.0.1.1 255.255.255.0  
    nat inbound 2000 address-group 1 no-pat reversible  
    nat outbound 2000 address-group 2  
#  
ip route-static 202.38.1.2 32 GigabitEthernet1/2 10.0.1.1  
#  
acl number 2000  
    rule 0 permit source 192.168.1.0 0.0.0.255  
#  
nat address-group 1  
    address 202.38.1.2 202.38.1.2  
#  
nat address-group 2  
    address 202.38.1.3 202.38.1.3  
#
```

## 関連ドキュメント

- [H3C MSRシリーズルーターレイヤ3 IPサービスコンフィギュレーションガイド\(V7\)](#)
- [H3C MSRシリーズルーターレイヤ3 IPサービスコマンドリファレンス\(V7\)](#)