内部 Web サーバをサポートするためのネットワーク アドレス変換およびスタティック ポート アドレス変換の設定

目次

概要

Cisco IOS® ネットワーク アドレス変換（NAT）は、IP アドレス管理の単純化と IP アドレスの節約を目的として設計されています。 インターネットに接続するために、未登録の IP アドレスを使用するプライベート IP のインターネットワークをイネーブルにします。 NAT は、2 つのネットワークを接続する Cisco ルータ上で動作し、パケットが別のネットワークに転送される前に、内部ネットワークのプライベート（Inside ローカル）アドレスをパブリック アドレス（Outside ローカル）に変換します。 この機能の一部として、ネットワーク全体に対して 1 つのアドレスだけを外部にアドバタイズするように、NAT を設定できます。 これにより、内部ネットワークは世界から効果的に隠蔽されます。 これにより、セキュリティが強化されます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

NAT の主要機能の 1 つはスタティック Port Address Translation (PAT) です。PAT は Cisco IOS の設定内では「オーバーロード」とも呼ばれます。 スタティック PAT は、ローカル アドレスとグローバル アドレスとの間で 1 対 1 のマッピングを可能にすることを目的として設計されています。 一般的にスタティック PAT は、パブリック ネットワークからのインターネット ユーザに、プライベート ネットワーク内の Web サーバへのアクセスを許可するために使用されます。

NAT の詳細については、「NAT テクニカル サポート ページ」を参照してください。

次のテーブルは、プライベート ネットワークで使用可能な IP アドレス空間の 3 つのブロックを示しています。 これらの特殊なネットワークの詳細については、RFC 1918 を参照してください。

IP アドレス空間	クラス
10.0.0.0 ~ 10.255.255.255 (10/8 プレフィクス)	**クラス A**
172.16.0.0 ~ 172.31.255.255 (172.16/12 プレフィクス)	**クラス B**
192.168.0.0 ~ 192.168.255.255 (192.168/16 プレフィクス)	**クラス C**

注: 最初のブロックは単一のクラス A ネットワーク番号、2 番目のブロックは 16 の連続するクラス B ネットワーク番号のセット、3 番目のブロックは 256 の連続するクラス C ネットワーク番号のセットです。

この例では、インターネット サービス プロバイダー (ISP) によって、DSL 加入者に単一の IP アドレス (171.68.1.1/24) のみが割り当てられます。 割り当てられた IP アドレスは一意の登録済み IP アドレスで、内部グローバル アドレスと呼ばれます。 この登録済み IP アドレスは、インターネットを閲覧するためにプライベート ネットワーク全体で使用されます。また、パブリック ネットワークからのインターネット ユーザも、プライベート ネットワーク内の Web サーバにアクセスするためにこの登録済み IP アドレスを使用します。

プライベート LAN (192.168.0.0/24) は、NAT ルータのイーサネット インターフェイスに接続しています。 このプライベート LAN には、複数台の PC と 1 台の Web サーバがあります。 NAT ルータは、これらの PC から受け取る未登録の IP アドレス (内部ローカル アドレス) を、インターネット閲覧するための単一のパブリック IP アドレス (内部グローバル - 171.68.1.1) に変換するように設定されています。

IP アドレス 192.168.0.5 (Web サーバ) は、プライベート アドレス空間内のアドレスであり、インターネットへの経路指定はできません。 パブリックのインターネット ユーザが Web サーバに到達するためにアクセス可能な IP アドレスは、171.68.1.1 だけです。 このため、NAT ルータは、IP アドレス 171.68.1.1、ポート 80 (ポート 80 はインターネット閲覧用) と 192.168.0.5、ポート 80 との間で 1 対 1 のマッピングを実行するように設定されます。 このマッピング機能により、パブリック側のインターネット ユーザが内部 Web サーバにアクセスできるようになります。

次のネットワーク トポロジと設定例は、Cisco 827、1417、SOHO77、および 1700/2600/3600 ADSL WIC に使用することができます。 このドキュメントでは、例として、Cisco 827 が使用されています。

設定

このセクションには、このドキュメントで説明している機能を設定する際に利用できる情報が記載されています。

注: このドキュメントで使用されるコマンドの追加情報については、IOS の「コマンド ルックアップ ツール」（登録ユーザ専用）を参照してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

Cisco 827

```
Current Configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
!
hostname 827
!
ip subnet-zero
no ip domain-lookup
!
bridge irb
!
interface Ethernet0
ip address 192.168.0.254 255.255.255.0
ip nat inside !--- This is the inside local IP address
and it is a private IP address. ! interface ATM0 no ip
address no atm ilmi-keepalive pvc 0/35 encapsulation
aal5snap ! bundle-enable dsl operating-mode auto bridge-
group 1 ! interface BVI1 ip address 171.68.1.1
255.255.255.240 ip nat outside !--- This is the inside
global IP address. !--- This is your public IP address
and it is provided to you by your ISP. ! ip nat inside
source list 1 interface BVI1 overload !--- This
statement makes the router perform PAT for all the !---
End Stations behind the Ethernet interface that uses !--
- private IP addresses defined in access list #1. ip nat
inside source static tcp 192.168.0.5 80 171.68.1.1 80
extendable !--- This statement performs the static
address translation for the Web server. !--- With this
statement, users that try to reach 171.68.1.1 port 80
(www) are !--- automatically redirected to 192.168.0.5
port 80 (www). In this case !--- it is the Web server.
ip classless ip route 0.0.0.0 0.0.0.0 171.68.1.254 !---
IP address 171.68.1.254 is the next hop IP address, also
!--- called the default gateway. !--- Your ISP can tell
you what IP address to configure as the next hop
address. ! access-list 1 permit 192.168.0.0 0.0.0.255 !-
```

```
-- This access list defines the private network !---
that is network address translated. bridge 1 protocol
ieee bridge 1 route ip ! end
```

確認

show ip nat translation コマンドの出力中にある Inside local は、内部ネットワーク上の Web サーバに割り当てられた設定済みの IP アドレスです。 192.168.0.5 はプライベート アドレス空間内のアドレスであり、インターネットへの経路指定はできません。 Inside global は内部ホストの IP アドレスであり、外部ネットワークに表示される Web サーバです。 これは、インターネットから Web サーバにアクセスするユーザが知ることのできるアドレスです。

Outside local は、内部ネットワークに表示される外部ホストの IP アドレスです。 必ずしも正規のアドレスとは限らず、 内部で経路指定可能なアドレス空間から割り当てられます。

Outside global アドレスは、ホストの所有者によって外部ネットワークのホストに割り当てられる IP アドレスです。 このアドレスは、グローバルに経路指定できるアドレス空間またはネットワーク空間から割り当てられます。

アドレス 171.68.1.1、ポート番号 80 (HTTP) は、192.168.0.5、ポート 80 に変換されます (逆の変換も同様に行われます) 。 したがってインターネット ユーザは、Web サーバがプライベート ネットワーク上のプライベート IP アドレスにあっても、Web サーバを閲覧できます。

NAT のトラブルシューティング方法の詳細については、「NAT オペレーションの検証と NAT の基本的なトラブルシューティング」を参照してください。

```
827#
827#show ip nat translation Pro Inside global Inside local Outside local Outside global tcp
171.68.1.1:80 192.168.0.5:80 --- --- tcp 171.68.1.1:80 192.168.0.5:80 198.133.219.1:11000
198.133.219.1:11000 827#
```

トラブルシューティング

アドレス 変換を解決するために、アドレスが正しく変換するかどうか見るルータの **term mon** および **debug ip nat detailed コマンドを**発行できます。 外部ユーザが Web サーバに到達するためにアクセス可能な IP アドレスは、171.68.1.1 です。 たとえば、インターネットのパブリック側から 171.68.1.1、ポート 80 (www) に到達しようとしているユーザは、自動的に 192.168.0.5、ポート 80 (www) にリダイレクトされます。この場合、リダイレクト先は Web サーバです。

```
827#term mon 827#debug ip nat detailed IP NAT detailed debugging is on 827# 03:29:49: NAT:
creating portlist proto 6 globaladdr 171.68.1.1 03:29:49: NAT: Allocated Port for 192.168.0.5 ->
171.68.1.1: wanted 80 got 80 03:29:49: NAT: o: tcp (198.133.219.1, 11000) -> (171.68.1.1, 80)
[0] <... snipped ...>
```

関連情報

- Cisco DSL テクノロジーのサポート情報
- 製品サポート情報
- テクニカルサポートとドキュメント - Cisco Systems