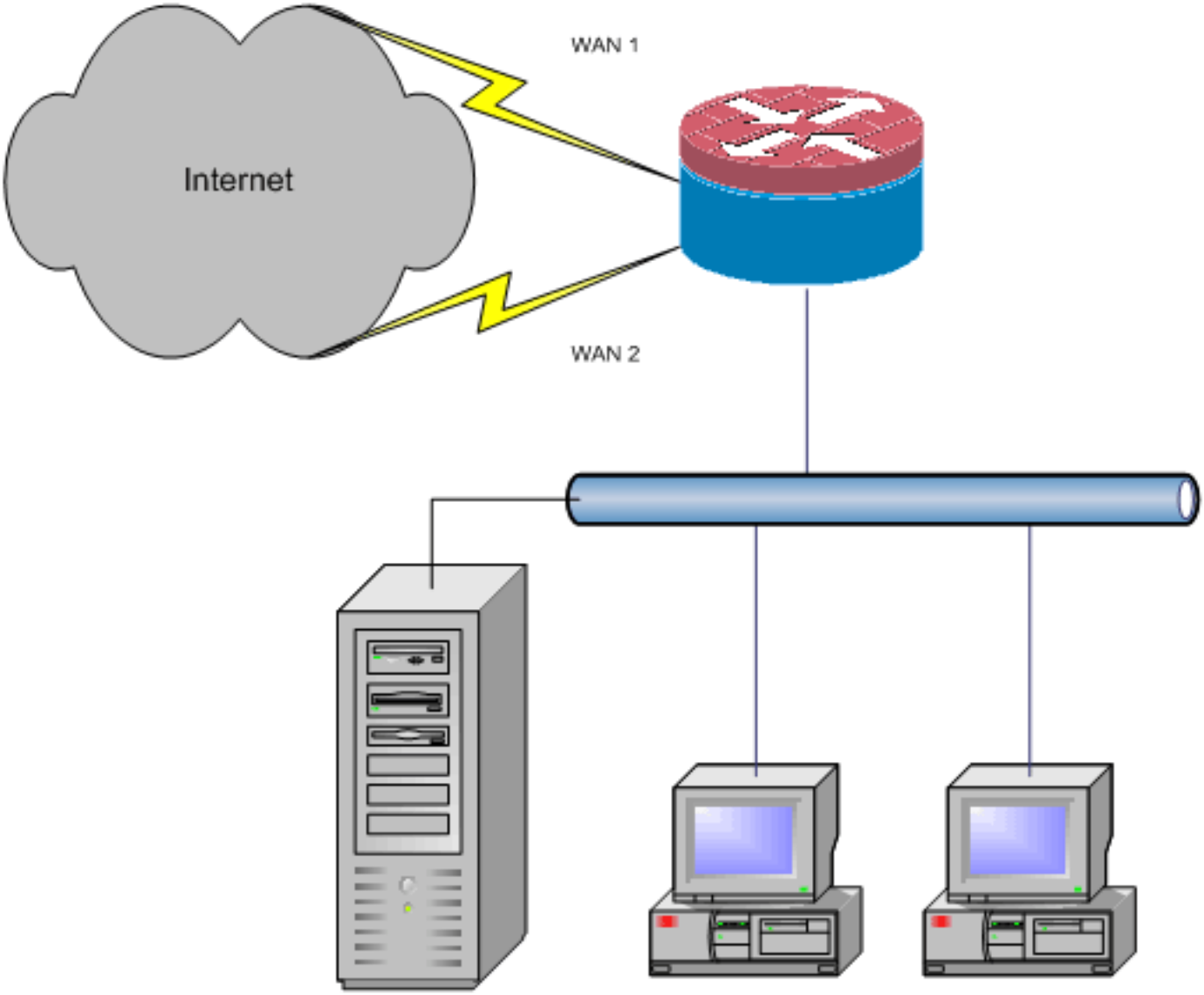
OERを使用した2つのISP接続用のCisco IOS NATの設定

内容

概要

このドキュメントでは、2つのISP接続を介してネットワークアドレス変換(NAT)を使用してネットワークをインターネットに接続するためのCisco IOS®ルータの設定について説明します。Cisco IOS NATは、特定の宛先への等コストルートが使用可能な場合、複数のネットワーク接続を介して後続のTCP接続とUDPセッションを配信できます。接続の1つが使用不能になった場合、オブジェクトトラッキング(Optimized Edge Routing(OER)のコンポーネント)を使用して、接続が再び使用可能になるまでルートを非アクティブ化し、ネットワークの可用性がインターネット接続の不安定性または信頼性を確実にします。



このドキュメントでは、NATによって提供される基本的なネットワーク保護を強化するステートフルインスペクション機能を追加するために、Cisco IOSゾーンベースポリシーファイアウォールを適用するための追加設定について説明します。

前提条件

要件

このドキュメントでは、すでにLANおよびWAN接続が機能しており、初期接続を確立するための設定やトラブルシューティングの背景が提供されていないことを前提としています。

このドキュメントでは、ルートを区別する方法については説明していません。したがって、望ましくない接続よりも望ましい接続を優先する方法はありません。

このドキュメントでは、ISPのDNSサーバの到達可能性に基づいていずれかのインターネットルートベースを有効または無効にするためにOERを設定する方法について説明します。1つのISP接続からのみ到達可能で、そのISP接続が使用できない場合に使用できない可能性がある特定のホストを特定する必要があります。

使用するコンポーネント

この設定は、12.4(15)T2 Advanced IP Servicesソフトウェアが稼働するCisco 1811ルータで開発されました。別のソフトウェアバージョンを使用している場合、一部の機能が使用できない場合、または設定コマンドがこのドキュメントに示されているコマンドと異なる場合があります。インターフェイスの設定はプラットフォームによって異なる可能性がありますが、すべてのCisco IOSルータプラットフォームで同様の設定を使用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『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。

設定

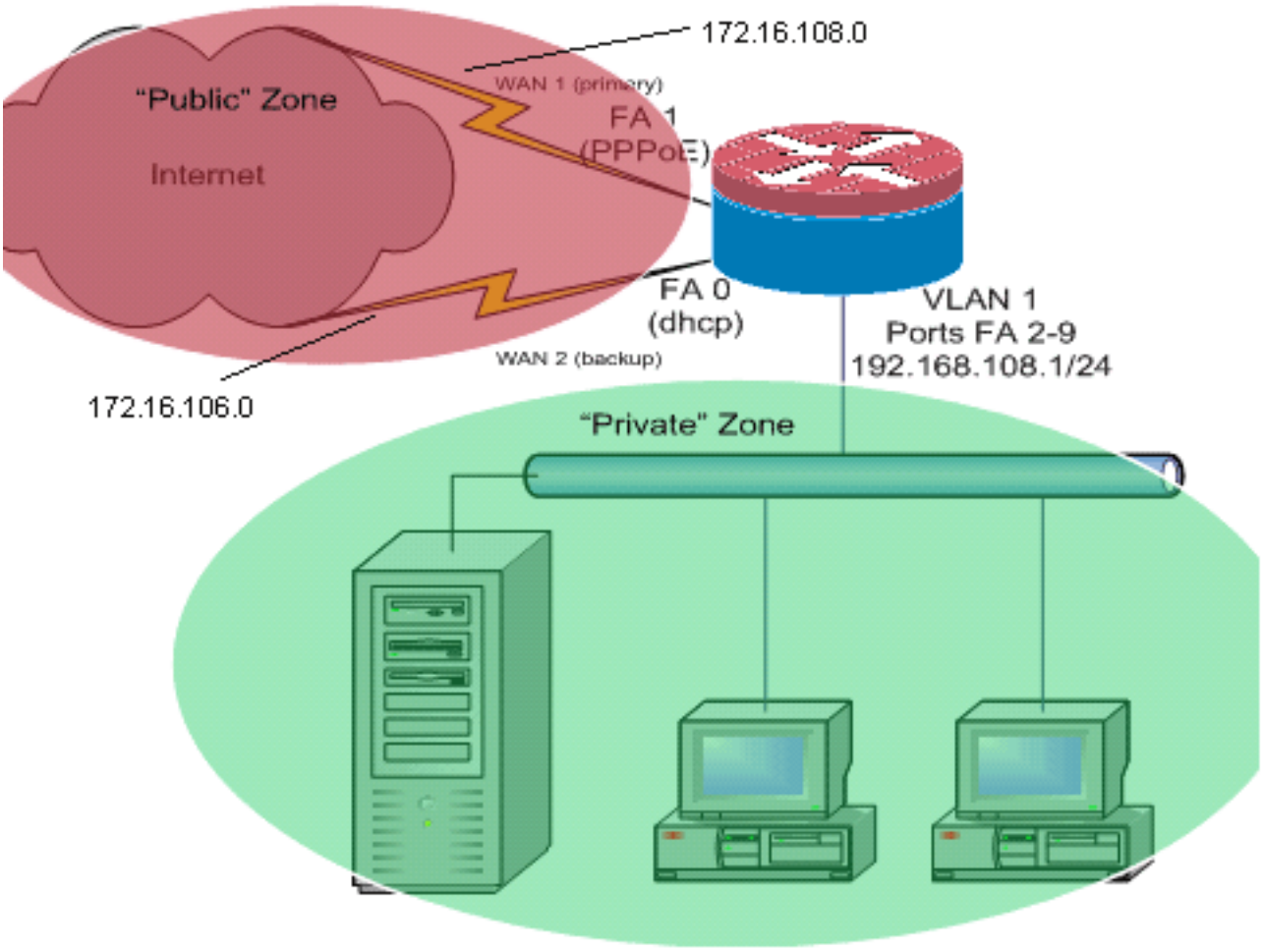
特定のトラフィックにポリシーベースルーティングを追加して、常に1つのISP接続を使用するようにすることが必要になる場合があります。この動作を必要とするトラフィックの例としては、IPsec VPNクライアント、VoIPハンドセット、および接続で同じIPアドレス、高速、または低遅延を優先するために常に1つのISP接続オプションのみを使用する必要があるその他のトラフィックがあります。

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

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 セットアップを使用します。



この設定例は、ネットワークダイアグラムに示されているように、1つのISP（FastEthernet 0で示される）へのDHCPで設定されたIP接続と、もう1つのISP接続を介したPPPoE接続を使用するアクセスルータについて説明しています。オブジェクトトラッキングと最適化エッジルーティング(OER)またはポリシーベースルーティングをDHCP割り当てのインターネット接続で使用しない限り、接続タイプは設定に特に影響しません。このような場合、ポリシールーティングまたはOER用のネクストホップルータを定義することは非常に困難である可能性があります。

ファイアウォール ポリシーの説明

この設定例では、「内部」セキュリティゾーンから「外部」セキュリティゾーンへの単純なTCP、UDP、およびICMP接続を許可し、発信FTP接続とアクティブとパッシブの両方のFTP転送に対応するデータトラフィックを格納するファイアウォールポリシーについて説明します。この基本ポリシーで処理されない複雑なアプリケーショントラフィック（VoIPシグナリングやメディアなど）は、機能が低下した状態で動作するか、完全に失敗する可能性があります。このファイアウォールポリシーは、「パブリック」セキュリティゾーンから「プライベート」ゾーンへのすべての接続をブロックします。これには、NATポート転送によって対応されるすべての接続が含まれます。この基本設定で処理されない追加のトラフィックに対応するには、追加のファイアウォールポリシー設定を構築する必要があります。

ゾーンベースポリシーファイアウォールのポリシーの設計と設定に関する質問がある場合は、『ゾーンベースポリシーファイアウォールの設計とアプリケーションガイド』を参照してください。

CLI での設定

Cisco IOS CLIの設定

```
track timer interface 5
!
!
track 123 rtr 1 reachability
 delay down 15 up 10
!
track 345 rtr 2 reachability
 delay down 15 up 10
!
!---Configure timers on route tracking class-map type
inspect match-any priv-pub-traffic match protocol ftp
match protocol tcp match protocol udp match protocol
icmp ! policy-map type inspect priv-pub-policy class
type inspect priv-pub-traffic inspect class class-
default ! zone security public zone security private
zone-pair security priv-pub source private destination
public service-policy type inspect priv-pub-policy ! !
interface FastEthernet0 ip address dhcp ip dhcp client
route track 345
 ip nat outside
 ip virtual-reassembly
 zone security public
!
!---Use "ip dhcp client route track [number]" !--- to
monitor route on DHCP interfaces !--- Define ISP-facing
interfaces with "ip nat outside" interface FastEthernet1
no ip address pppoe enable no cdp enable ! interface
FastEthernet2 no cdp enable ! interface FastEthernet3 no
cdp enable ! interface FastEthernet4 no cdp enable !
interface FastEthernet5 no cdp enable ! interface
FastEthernet6 no cdp enable ! interface FastEthernet7 no
cdp enable ! interface FastEthernet8 no cdp enable !
interface FastEthernet9 no cdp enable ! ! interface
Vlan1 description LAN Interface ip address 192.168.108.1
255.255.255.0 ip nat inside ip virtual-reassembly ip tcp
adjust-mss 1452 zone security private !--- Define LAN-
facing interfaces with "ip nat inside" ! ! Interface
Dialer 0 description PPPoX dialer ip address negotiated
ip nat outside ip virtual-reassembly ip tcp adjust-mss
zone security public !---Define ISP-facing interfaces
with "ip nat outside" ! ip route 0.0.0.0 0.0.0.0 dialer
0 track 123 ! ! ip nat inside source route-map fixed-nat
interface Dialer0 overload ip nat inside source route-
map dhcp-nat interface FastEthernet0 overload !---
Configure NAT overload (PAT) to use route-maps ! ! ip
sla 1 icmp-echo 172.16.108.1 source-interface Dialer0
timeout 1000 threshold 40 frequency 3 !---Configure an
OER tracking entry to monitor the !---first ISP
connection ! ! ! ip sla 2 icmp-echo 172.16.106.1 source-
interface FastEthernet0 timeout 1000 threshold 40
frequency 3 !--- Configure a second OER tracking entry
to monitor !---the second ISP connection ! ! ! ip sla
schedule 1 life forever start-time now ip sla schedule 2
life forever start-time now !---Set the SLA schedule and
duration ! ! ! access-list 110 permit ip 192.168.108.0
0.0.0.255 any !--- Define ACLs for traffic that will be
!--- NATed to the ISP connections ! ! ! route-map fixed-
nat permit 10 match ip address 110 match interface
Dialer0 ! route-map dhcp-nat permit 10 match ip address
110 match interface FastEthernet0 !--- Route-maps
associate NAT ACLs with NAT !--- outside on the ISP-
facing interfaces
```

dhcp割り当てルートトラッキングを使用します。

Cisco IOS CLIの設定
interface FastEthernet0 description Internet Intf ip dhcp client route track 123 ip address dhcp ip nat outside ip virtual-reassembly speed 100 full-duplex no cdp enable

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show ip nat translation：NAT Inside ホストと NAT Outside ホストの間の NAT アクティビティを表示します。**このコマンドを使用すると、Inside ホストが両方の NAT Outside アドレスに変換されることを確認できます。

```
Router#show ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.108.44:54486 192.168.108.3:54486 172.16.104.10:22 172.16.104.10:22
tcp 172.16.106.42:49620 192.168.108.3:49620 172.16.102.11:80 172.16.102.11:80
tcp 172.16.108.44:1623 192.168.108.4:1623 172.16.102.11:445  172.16.102.11:445
Router#
```

- **show ip route：インターネットへのルートが複数存在することを確認します。**

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.108.1 to network 0.0.0.0

C    192.168.108.0/24 is directly connected, Vlan1
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.108.0 is directly connected, FastEthernet4
C       172.16.106.0 is directly connected, Vlan106
S*   0.0.0.0/0 [1/0] via 172.16.108.1
                [1/0] via 172.16.106.1
```

- **show policy-map type inspect zone-pair sessions**：プライベートゾーンホストとパブリックゾーンホスト間のファイアウォール検査アクティビティを表示します。このコマンドは、ホストが外部セキュリティゾーンのサービスと通信するときに、内部ホストのトラフィックが検査されることを確認します。

トラブルシュート

NATを使用してCisco IOSルータを設定した後に接続が機能しない場合は、次の項目を確認します。

- Outside インターフェイスと Inside インターフェイスで NAT が適切に適用されている。
- NAT 設定が完全であり、NAT を適用する必要があるトラフィックが ACL に反映されている。
- インターネットおよび WAN への利用可能なルートが複数存在する。
- ルートトラッキングを使用する場合は、インターネット接続が使用可能であることを確認するために、ルートトラッキングの状態を確認します。
- ファイアウォール ポリシーが、ルータの通過を許可するトラフィックの特性を正確に反映している。

関連情報

- Cisco IOS ファイアウォール
- Cisco IOS IPアドレッシングサービスコマンドリファレンス – NATコマンド
- ゾーンベース ポリシー ファイアウォールの設計と適用ガイド
- Cisco IOS Optimized Edge Routingコンフィギュレーションガイド、リリース12.4T
- テクニカル サポートとドキュメント – Cisco Systems