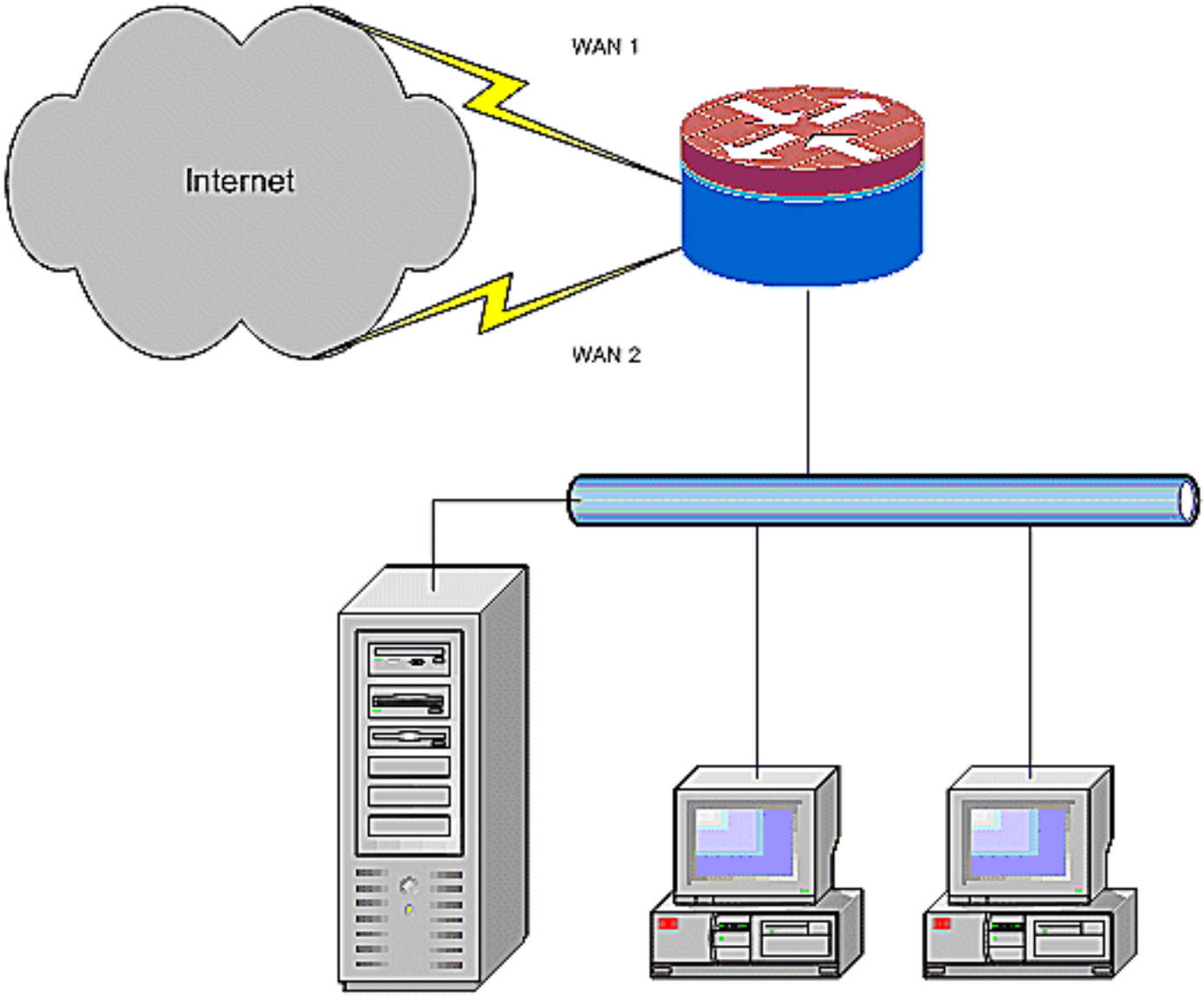
2 つの IPS 接続に対するゾーンベース ポリシー ファイアウォールを使用した IOS NAT ロード バランシング

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®ルータの設定例を紹介します。Cisco IOS ソフトウェアの NAT では、特定の宛先までの等コスト ルートが複数ある場合、複数のネットワーク接続を介して後続の TCP 接続および UDP セッションを分散できます。



このドキュメントでは、Cisco IOS Zone-Based ポリシー ファイアウォール（ZFW）を適用してステートフル インスペクション機能を追加し、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追加の設定を示します。

前提条件

要件

このドキュメントは、LAN および WAN 接続で作業していることを前提としています。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に関する情報は提供していません。このドキュメントでは、ルート間で差別化を行う方法については説明していないので、一方の接続を他方の接続よりも優先的に使用する方法は記載されていません。

使用するコンポーネント

このドキュメントの情報は、12.4(15) T3 高度 IP サービス ソフトウェアを使用する Cisco 1811 シリーズ ルータに基づきます。他のソフトウェア バージョンを使用する場合は、一部の機能を使

用できない場合や、コンフィギュレーション 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。同様の設定はすべての Cisco IOS ルータ プラットフォームで使用できますが、多くの場合、インターフェイス設定はプラットフォームごとに異なります。

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

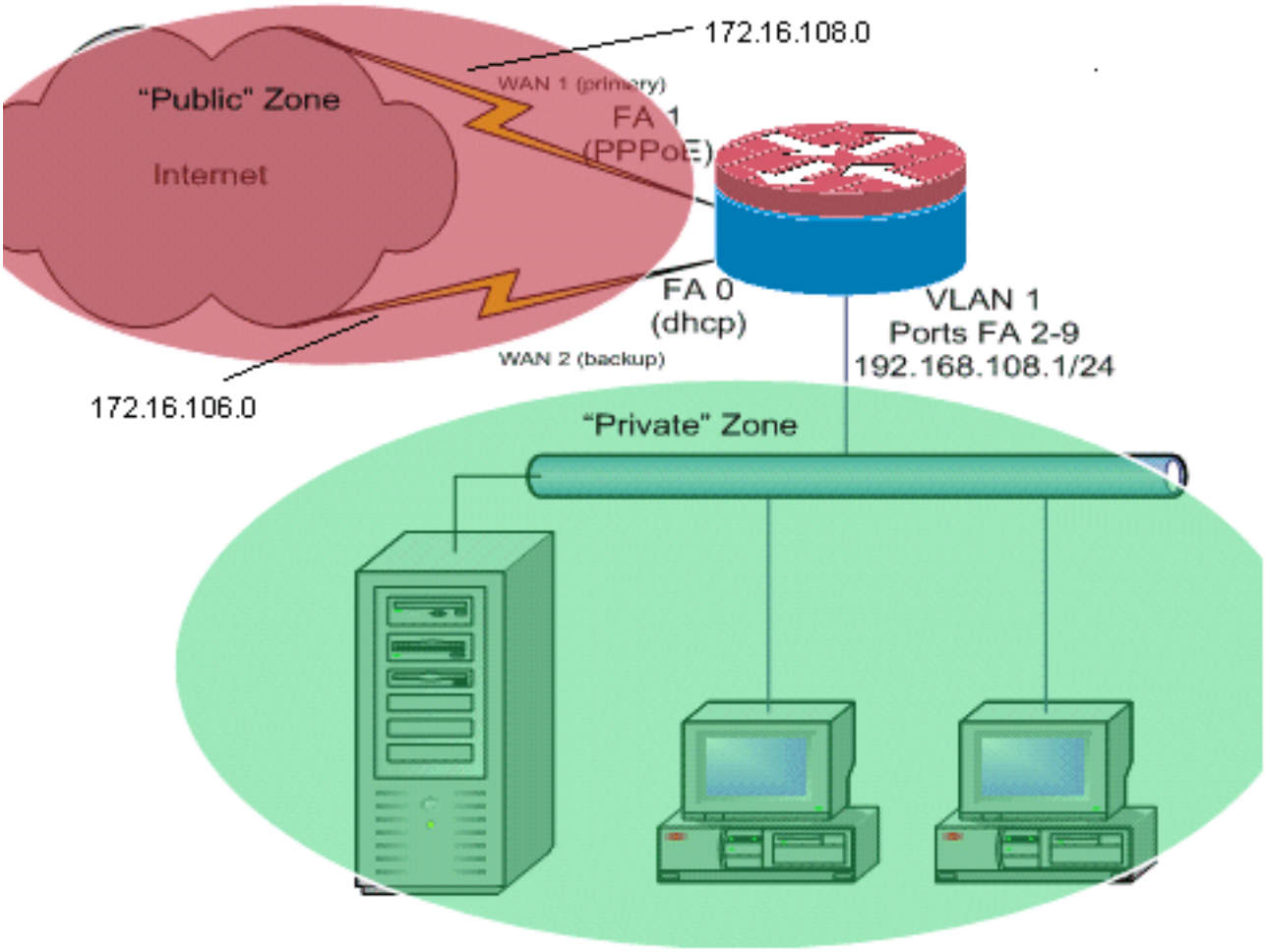
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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。

特定のトラフィックが常に 1 つの ISP 接続を使用するようにするには、ポリシーベース ルーティングを追加する必要がある場合があります。この動作を必要とするトラフィックの例には、IPSec VPN クライアント、VoIP テレフォニー トラフィック、および 1 つの ISP 接続オプションのみを使用して同じ IP アドレスに高速かつ低遅延で到達するその他のトラフィックが含まれます。

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。



この設定例では、（FastEthernet 0 で示される）1 つの ISP への DHCP 対応の IP 接続と、他の ISP 接続を経由する 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。接続タイプは設定に特定の影響を及ぼしませんが、一部の接続タイプが特定の失敗のシナリオでこの設定の有用性を妨げることがあります。これは特に、イーサネット接続された WAN サービス経由の IP 接続が使用されている場合、たとえば、追加デバイスが WAN 接続を終端しイーサネットを Cisco IOS ルータへ引き渡すようなケーブル モデムや DSL サービスで顕著です。DHCP 割り当てアドレスや PPPoE とは逆に、静的 IP アドレッシングが適用され、イーサネット ポートが WAN 接続デバイスへのイーサネット リンクを留保してしまうといった WAN 障害が発生した場合、ルータは継続して正常な WAN 接続と不良な WAN 接続の両方に接続のロード バランスを試みます。展開の中で、非アクティブなルートをロード バランシングの対象から削除する必要がある場合は、ルートの妥当性を監視するための Optimized Edge Routing の追加について説明したドキュメント「2 つのインターネット接続に対して Optimized Edge Routing を使用する Cisco IOS NAT ロード バランシングとゾーンベース ポリシー ファイアウォール」に掲載されている設定を参照してください。

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、アウトバウンド FTP 接続と、アクティブおよびパッシブ両方の FTP 転送に対する同等のデータ トラフィックに対応するファイアウォール ポリシーについて説明しています。この基本ポリシーで処理されない、VoIP シグナリングおよびメディアなどの複雑なアプリケーション トラフィックは、機能が制限されたり、完全に失敗したり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。必要に応じてファイアウォール インスペクション ポリシーを調整し、アプリケーション プロファイルおよびセキュリティ ポリシーに合わせる必要があり

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設計と設定についてわからないことがある場合は、「ゾーンベース ポリシー ファイアウォール設計およびアプリケーション ガイド」を参照してください。

設定

このドキュメントでは、次の構成を使用します。

コンフィギュレーション

```
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 nat outside ip virtual-
reassembly zone security public ! interface
FastEthernet1 no ip address pppoe enable no cdp enable !
interface FastEthernet2 no cdp enable !--- Output
Suppressed 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 ! 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 ! 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
```

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 translation
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 インスペクション 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、ホストが「Outside」セキュリティ ゾーン内のサービスと通信するときに Inside ホストのトラフィックが検査されていることを検証できます。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco IOS ルータで NAT をした後に接続が機能しない場合は、次のことを確認してください。

- 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。
- 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

- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- Cisco IP Telephony のトラブルシューティング
- 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
- テクニカル サポートとドキュメント – Cisco Systems