Optimized Edge Routing を使用した 2 つのインターネット接続に対する IOS NAT ロード バランシングおよびゾーンベース ポリシー ファイアウォール

目次

概要

この資料は 2 つの ISP 接続によってネットワーク アドレス変換（NAT）とインターネットにネットワークを接続するために Cisco IOS® ルータのための設定を説明したものです。 Cisco IOS NAT は所定のデスティネーションへの等コスト ルートが利用できる場合マルチプルネットワーク接続上のそれに続く TCP 接続および UDP セッションを配ることができます。 接続の 1 つが使用不可能になれば、不安定な状態にもかかわらずネットワークアベイラビリティかインターネット接続の不信頼性を確認する接続が再度利用可能になるまでオブジェクト トラッキングが、Optimized Edge Routing （OER）のコンポーネント、ルートを無効にするのに使用することができます。

この資料は NAT によって提供される基本的なネットワーク保護を増加するためにステートフル点検機能を追加するように Cisco IOS ゾーン ベースのポリシー ファイアウォールを適用するように追加コンフィギュレーションを説明したものです。

前提条件

要件

この資料はまだはたらくあり、最初の接続を確立するために設定かトラブルシューティング バックグラウンドを提供していないことを LAN および WAN 接続が仮定します。

この資料はルーティングを区別する方法を記述しないものです。 従って、より少なく好ましい接続上のより好ましい接続を好む方法がありません。

この資料に ISP の DNSサーバの到達可能性でルート ベースのどちらかのインターネットを有効に するか、またはディセーブルにするために OER を設定する方法を記述されています。 その ISP 接続が利用できない場合 ISP 接続の 1 だけによって到達可能、利用可能ではないかもしれない特定のホストを識別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 によって進められる IP サービス ソフトウェアを実行する Cisco 1811 ルータによって作成されました。 別のソフトウェア バージョンが使用される場合、いくつかの機能は利用可能ではないかもしれませんまたは設定コマンドはこの資料で示されているそれらと異なるかもしれません。 同じようなコンフィギュレーションはインターフェイスコンフィギュレーションが異なるプラットフォームの間で多分変わるがすべての Cisco IOS ルータ プラットフォームで利用可能であるはずです。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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

1 つの ISP 接続を常に使用することを確かめるために特定のトラフィックのためのポリシー ベース ルーティングを追加する必要があるかもしれません。 この動作を必要とするかもしれないトラフィックの例は IPSec VPN クライアント、VoIP 受話器をおよび接続の同じ IP アドレス、より高い速度、またはより低いレイテンシーを好む ISP 接続オプションの 1 つだけを常に使用する必要がある他のどのトラフィックも含まれています。

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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）を使用してください。

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。

FastEthernet によって 0）示されているこの設定例は、ネットワークダイアグラムに示すように、1 ISP に DHCP 設定された IP接続を使用するアクセスルータを説明します（および他の ISP 接続上の PPPoE 接続。 オブジェクト トラッキングおよび Optimized Edge Routing （OER）および/またはポリシー ベース ルーティングが DHCP 割り当て インターネット接続と使用されるべきなら、接続タイプに設定の特定の影響がありません。 このような場合、ポリシー ルーティングまたは OER のためのネクストホップ ルータを定義することは非常に困難かもしれません。

ファイアウォール ポリシーの説明

「内部」セキュリティ ゾーンからの「外部」セキュリティ ゾーンへの簡単な TCP、UDP および ICMP 接続を可能にし、両方のアクティブおよびパッシブFTP 転送のための FTP 送信接続および対応 する データ トラフィックに対応するこの設定例はファイアウォール ポリシーを記述します。 どの複雑なアプリケーショントラフィックでも減少された機能で（たとえば、VoIP シグナリングおよびメディア）この基本的 な ポリシーによって処理されない多分動作するか、または完全に失敗するかもしれません。 このファイアウォール ポリシーは「公共」セキュリティ ゾーンからの NATポート フォワーディングによって取り扱われるすべての接続を含む「私用」ゾーンへのすべての接続をブロックします。 この基本設定によって処理されない追加トラフィックに対応するために追加ファイアウォール ポリシー 設定を組み立てて下さい。

ゾーン ベースのポリシー ファイアウォール政策設計および設定の質問がある場合、ゾーン ベースのポリシー ファイアウォール 設計およびアプリケーション ガイドを参照して下さい。

CLI 設定

Cisco IOS CLI 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て下さい:

Cisco IOS CLI 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、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **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 タイプ Inspect ゾーン ペアは sessions — private** 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する。 この

コマンドはホストが国外安全保証 ゾーンのサービスと通信すると同時に内部ホストのトラフィックが検査されること確認を提供したものです。

トラブルシューティング

NAT で Cisco IOS ルータを設定した後接続がはたらかない場合これらの項目を確認して下さい:

- 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。
- トラッキングするルートを使用する場合インターネット接続を確認するためにトラッキングするルートの状態をです利用可能チェックして下さい。
- 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
- サービスにコマンドレファレンス 当たる Cisco IOS IP - 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アプリケーション 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