



トラフィック ゾーン

トラフィックゾーンに複数のインターフェイスを割り当てることができます。これにより、既存のフローのトラフィックがゾーン内のインターフェイスで ASA に出入りできるようになります。この機能により、ASA 上での等コストマルチパス (ECMP) のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。

- [トラフィック ゾーンの概要 \(1 ページ\)](#)
- [トラフィック ゾーン的前提条件 \(8 ページ\)](#)
- [トラフィック ゾーンのガイドライン \(10 ページ\)](#)
- [トラフィック ゾーンの設定 \(11 ページ\)](#)
- [トラフィック ゾーンのモニタリング \(12 ページ\)](#)
- [トラフィック ゾーンの例 \(15 ページ\)](#)
- [トラフィック ゾーンの履歴 \(18 ページ\)](#)

トラフィック ゾーンの概要

この項では、ネットワークでトラフィックゾーンを使用する方法について説明します。

ゾーン分割されていない動作

アダプティブセキュリティアルゴリズムは、トラフィックの許可または拒否を決定する際に、パケットの状態を考慮します。フローに適用されたパラメータの1つは、トラフィックが同じインターフェイスに出入りすることです。異なるインターフェイスに入る既存のフローのトラフィックは、ASA によってドロップされます。

トラフィックゾーンにより、複数のインターフェイスを1つにまとめることができるため、ゾーン内の任意のインターフェイスに出入りするトラフィックがアダプティブセキュリティアルゴリズムのセキュリティチェックを満たすことができます。

関連トピック

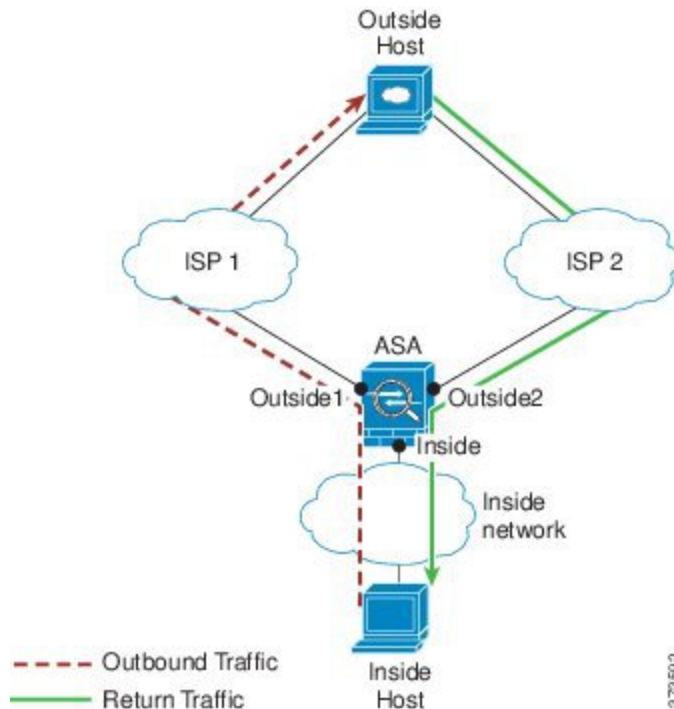
[ステートフルインスペクションの概要](#)

ゾーンを使用する理由

ゾーンを使用して、複数のルーティングのシナリオに対応することができます。

非対称ルーティング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。宛先ネットワークの非対称ルーティングが原因で、Outside2 インターフェイスの ISP 2 からリターン トラフィックが到達しています。

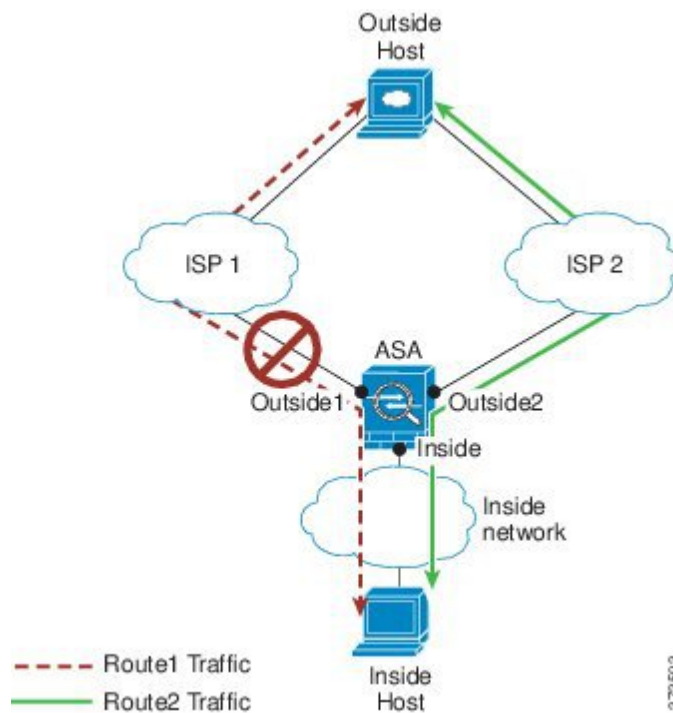


ゾーン分割されていない場合の問題：ASAは、インターフェイスごとに接続テーブルを保持します。リターン トラフィックが Outside2 に到達すると、そのトラフィックは、接続テーブルに一致しないため、ドロップされます。ASA クラスタに関しては、クラスタが同一ルータに対して複数の隣接関係（アジャセンシー）を持つ場合、非対称ルーティングは許容できないトラフィック紛失の原因となることがあります。

ゾーン分割されたソリューション：ASAは、ゾーンごとに接続テーブルを保持します。Outside1 と Outside2 を 1 つのゾーンにグループ化した場合、リターン トラフィックが Outside2 に到達すると、ゾーンごとの接続テーブルに一致するため、接続が許可されます。

紛失したルート

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。Outside1 と ISP 1 間でルートが紛失または移動したため、トラフィックは ISP 2 を経由する別のルートを通る必要があります。

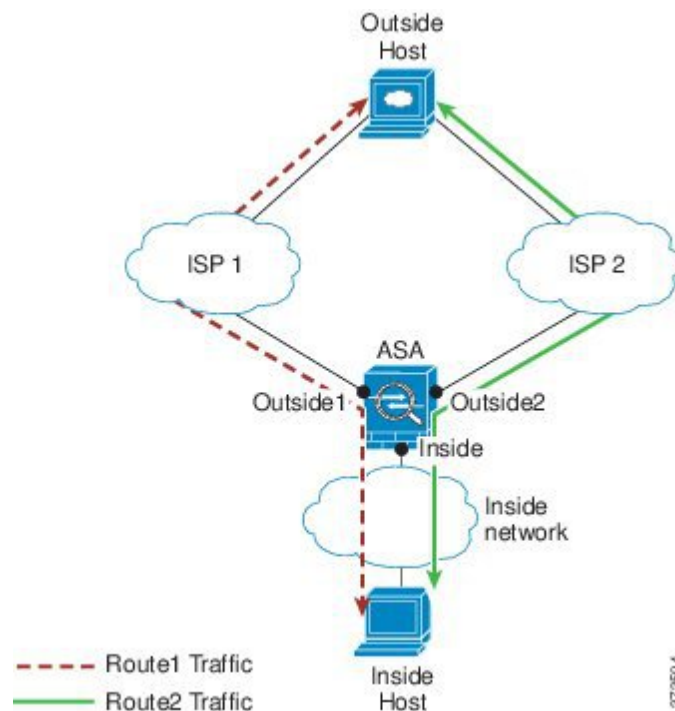


ゾーン分割されていない場合の問題：内部ホストと外部ホスト間の接続が削除されるため、新しい次善のルートを使用して新しい接続を確立する必要があります。UDP の場合、1 つのパケットがドロップダウンすると新しいルートが使用され、UDP がない場合は、新しい接続を再確立する必要があります。

ゾーン分割されたソリューション：ASA は、紛失したルートを検出し、フローを ISP 2 経由の新しいパスに切り替えます。トラフィックは、パケットがドロップすることなくシームレスに転送されます。

ロード バランシング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。2 番目の接続が Outside2 の ISP 2 を経由する等コスト ルートを介して確立されています。



ゾーン分割されていない場合の問題： インターフェイス間でロードバランシングを行うことができません。可能なのは、1つのインターフェイスの等コストルートによるロードバランスだけです。

ゾーン分割されたソリューション： ASAは、ゾーン内のすべてのインターフェイスで最大8つの等コストルート間の接続をロードバランスすることができます。

ゾーンごとの接続テーブルおよびルーティング テーブル

ASAは、トラフィックがゾーンのインターフェイスのいずれかに到達できるようにゾーンごとの接続テーブルを保持します。また、ASAは、ECMPサポート用にゾーンごとのルーティング テーブルも保持します。

ECMP ルーティング

ASA では、等コスト マルチパス（ECMP）ルーティングをサポートしています。

ゾーン分割されていない ECMP サポート

ゾーンがない場合は、インターフェイスごとに最大8つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスに3つのデフォルト ルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
```

```
route outside 0 0 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロード バランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMPは複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route outside2 0 0 10.2.1.1
```

ゾーン分割された ECMP サポート

ゾーンがある場合は、ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイス間に 3 つのデフォルト ルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、自動的に等コスト ルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス全体でトラフィックをロード バランスします。

ルートが紛失した場合、ASA はフローをシームレスに別のルートに移動させます。

接続のロード バランス方法

ASA では、パケットの 6 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル、入力インターフェイス）から生成されたハッシュを使用して、等コスト ルート間の接続をロード バランスします。ルートが紛失しない限り、接続は接続期間中、インターフェイスで継続されます。

接続内のパケットは、ルート間でロード バランスされません。接続では、そのルートが紛失しない限り、単一ルートを使用します。

ASA では、ロード バランシング時にインターフェイス帯域幅やその他のパラメータを考慮しません。同じゾーン内のすべてのインターフェイスが MTU、帯域幅などの同じ特性を持つことを確認します。

ロード バランシング アルゴリズムは、ユーザ設定可能ではありません。

別のゾーンのルートへのフォールバック

ルートがインターフェイスで紛失したときにゾーン内で使用可能な他のルートがない場合、ASA では、異なるインターフェイス/ゾーンからのルートを使用します。このバックアップ

ルートを使用した場合、ゾーン分割されていないルーティングのサポートと同様にパケットのドロップが発生することがあります。

インターフェイスベースのセキュリティ ポリシーの設定

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。必須の平行インターフェイス設定の詳細については、[トラフィック ザーンの前提条件（8 ページ）](#)を参照してください。

トラフィック ザーンでサポートされるサービス

次のサービスがゾーンでサポートされています。

- アクセル ルール
- NAT
- QoS トラフィック ポリシングを除くサービス ルール。
- Routing

完全にゾーン分割されたサポートは利用できませんが、[To-the-Box](#) および [From-the-Box](#) [トラフィック（7 ページ）](#) に示した to-the-box サービスおよび from-the-box サービスを設定することもできます。

トラフィック ザーンのインターフェイスに他のサービス（VPN、ボットネット トラフィック フィルタなど）を設定しないでください。これらのサービスは、想定どおりに機能または拡張しないことがあります。



（注） セキュリティ ポリシーの設定方法の詳細については、[トラフィック ザーンの前提条件（8 ページ）](#)を参照してください。

セキュリティ レベル

ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

フローのプライマリおよび現在のインターフェイス

各接続フローは、最初の入出力インターフェイスに基づいて構築されます。これらのインターフェイスは、プライマリ インターフェイスです。

ルート変更または非対称ルーティングにより、新しい出力インターフェイスが使用されている場合は、新しいインターフェイスが現在のインターフェイスになります。

ゾーンの追加または削除

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

ゾーン内トラフィック

トラフィックがあるインターフェイスに入り、同じゾーンの別のインターフェイスから出ることができるようにするには、**same-security permit intra-interface** コマンドをイネーブルにしてトラフィックが同じインターフェイスを出入りできるようにし、さらに、**same-security permit inter-interface** コマンドをイネーブルにして **same-security** インターフェイス間のトラフィックを許可します。このように設定しない場合、フローは同じゾーンの2つのインターフェイス間をルーティングできません。

To-the-Box および From-the-Box トラフィック

- **management-only** インターフェイスまたは **management-access** インターフェイスをゾーンに追加することはできません。
- ゾーンの通常のインターフェイスでの管理トラフィックでは、既存のフローの非対称ルーティングのみがサポートされます。ECMP サポートはありません。
- 1つのゾーンインターフェイスにのみ管理サービスを設定できますが、非対称ルーティング サポートを利用するには、すべてのインターフェイスでそれを設定する必要があります。構成がすべてのインターフェイスでパラレルである場合でも、ECMPはサポートされません。
- ASA は、ゾーンで次の To-the-Box および From-the-Box サービスをサポートします。
 - Telnet
 - SSH
 - HTTPS
 - SNMP

- Syslog

ゾーン内の IP アドレスのオーバーラップ

ゾーン分割されていないインターフェイスの場合、ASA では、NAT が正しく設定されていれば、インターフェイスでの IP アドレス ネットワークのオーバーラップをサポートします。ただし、同じゾーンのインターフェイスでは、ネットワークのオーバーラップはサポートされていません。

トラフィック ザーンの前提条件

- 名前、IP アドレス、およびセキュリティレベルを含むすべてのインターフェイスパラメータを設定します。ゾーンのすべてのインターフェイスでセキュリティレベルが一致する必要がありますことに注意してください。帯域幅および他のレイヤ 2 のプロパティについては、インターフェイスのようにグループ化する計画を立てる必要があります。
- 次のサービスをゾーンのすべてのインターフェイスで一致するように設定します。
 - アクセス ルール：同じアクセス ルールをゾーンのすべてのメンバー インターフェイスに適用するか、グローバル アクセス ルールを使用します。

次に例を示します。

```
access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
access-group ZONE1 in interface outside1
access-group ZONE1 in interface outside2
access-group ZONE1 in interface outside3
```

- NAT：ゾーンのすべてのメンバー インターフェイスで同じ NAT ポリシーを設定するか、グローバル NAT ルールを使用します（つまり、「any」を使用して NAT ルールでゾーンのインターフェイスを表します）。

インターフェイス PAT はサポートされていません。

次に例を示します。

```
object network WEBSERVER1
  host 10.9.9.9 255.255.255.255
  nat (inside,any) static 209.165.201.9
```



- (注) インターフェイス固有の NAT および PAT プールを使用したときに元のインターフェイスの障害が発生した場合、ASAは接続を切り替えることはできません。

インターフェイス固有の PAT プールを使用する場合、同じホストからの複数の接続は、別のインターフェイスにロードバランスし、別のマッピング IP アドレスを使用することがあります。この場合、複数の同時接続を使用するインターネットサービスが正しく機能しないことがあります。

- サービス ルール：グローバル サービス ポリシーを使用するか、ゾーンの各インターフェイスに同じポリシーを割り当てます。

QoS トラフィック ポリシングはサポートされていません。

次に例を示します。

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```



- (注) VoIP インспекションでは、ゾーンのロード バランシングにより、順序が正しくないパケットが増加する可能性があります。この状況は、異なるパスを通る先行パケットの前に後行パケットが ASA に到達する可能性があるために発生することがあります。順序が正しくないパケットには、次のような症状があります。

- キューイングを使用した場合に、中間ノード（ファイアウォールと IDS）および受信エンドノードでメモリ使用率が高い。
- ビデオまたは音声の品質が低い。

これらの影響を軽減するには、VoIP トラフィックのロード分散にのみ IP アドレスを使用することを推奨します。

- ECMP ゾーン機能を考慮してルーティングを設定します。

トラフィック ゾーンのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードまたはルーテッド モードのブリッジグループ インターフェイスはサポートされません。

フェールオーバー

- フェールオーバー リンクまたはステート リンクをゾーンに追加することはできません。
- アクティブ/アクティブ フェールオーバー モードでは、各コンテキストのインターフェイスを非対称ルーティング (ASR) グループに割り当てることができます。このサービスにより、ピア装置の同様のインターフェイスに戻るトラフィックを元の装置に復元することができます。コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。ASR グループに関する詳細については、[非対称にルーティングされたパケットのサポートの設定 \(アクティブ/アクティブ モード\)](#) を参照してください。
- 各接続のプライマリ インターフェイスのみがスタンバイ装置に複製されます。現在のインターフェイスは複製されません。スタンバイ装置がアクティブになると、その装置によって必要に応じて現在の新しいインターフェイスが割り当てられます。

クラスタ

- クラスタ制御リンクをゾーンに追加することはできません。

その他のガイドライン

- 最大 256 ゾーンを作成できます。
- 次のタイプのインターフェイスをゾーンに追加できます。
 - 物理
 - VLAN
 - EtherChannel
 - Redundant
- 次のタイプのインターフェイスは追加できません。
 - 管理専用
 - 管理アクセス

- フェールオーバーまたはステート リンク
 - クラスタ制御リンク
 - EtherChannel インターフェイスまたは冗長インターフェイスのメンバーインターフェイス
 - VNI（さらに、通常のデータ インターフェイスが **nve** 専用としてマークされている場合、ゾーンのメンバーにすることはできません）
 - BVI、またはブリッジグループ メンバー インターフェイス。
-
- 1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。
 - ゾーンごとに最大 8 つのインターフェイスを含めることができます。
 - ECMP の場合、ゾーンのすべてのインターフェイス間で、ゾーンごとに最大 8 つの等コスト ルートを追加できます。また、8 ルート制限の一部として 1 つのインターフェイスに複数のルートを設定することもできます。
 - ゾーンにインターフェイスを追加すると、それらのインターフェイスのすべてのスタティック ルートが削除されます。
 - ゾーン内のインターフェイスで DHCP リレー を有効にできません。

トラフィック ゾーンの設定

名前を付けたゾーンを設定し、インターフェイスをそのゾーンに割り当てます。

手順

ステップ 1 ゾーンを追加します。

zone name

例 :

```
zone outside
```

ゾーン名は最大 48 文字です。

ステップ 2 インターフェイスをゾーンに追加します。

interface id zone-member zone_name

例 :

```
interface gigabitethernet0/0
  zone-member outside
```

ステップ3 インターフェイスをさらにゾーンに追加します。これらのインターフェイスのセキュリティレベルが、追加した最初のインターフェイスのセキュリティレベルと同じであることを確認します。

例：

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

例

次の例では、4つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

トラフィック ゾーンのモニタリング

この項では、トラフィック ゾーンをモニタする方法について説明します。

ゾーン情報

- **show zone** [*name*]

ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

show zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
Zone Member(s) : 2
  outside1      GigabitEthernet0/0
  outside2      GigabitEthernet0/1
```

- **show nameif zone**

インターフェイス名およびゾーン名を表示します。

show nameif zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show nameif zone
Interface                Name                zone-name          Security
GigabitEthernet0/0       inside-1            inside-zone        100
GigabitEthernet0/1.21    inside              inside-zone        100
GigabitEthernet0/1.31    4                  inside-zone        0
GigabitEthernet0/2       outside             outside-zone       0
Management0/0            lan                 outside-zone       0
```

ゾーン接続

- **show conn [long | detail] [zone zone_name [zone zone_name] [...]]**

show conn zone コマンドは、ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリ インターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。

show conn long zone コマンドの次の出力を参照してください。

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outsidel(outside2): 10.122.122.1:1080
inside-zone:insidel(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

デバッグ目的で高速セキュリティ パス テーブルを表示します。

- **show local-host [zone zone_name [zone zone_name] [...]]**

ゾーン内のローカル ホストのネットワーク状態を表示します。

show local-host zone コマンドについては、次の出力を参照してください。プライマリ インターフェイスが最初に表示され、現在のインターフェイスがカッコに囲まれています。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

Conn:
TCP outside-zone:outsidel(outside2): 10.122.122.1:1080
inside-zone:insidel(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

ゾーン ルーティング

• show route zone

ゾーン インターフェイスのルートを表示します。

show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

• show asp table routing

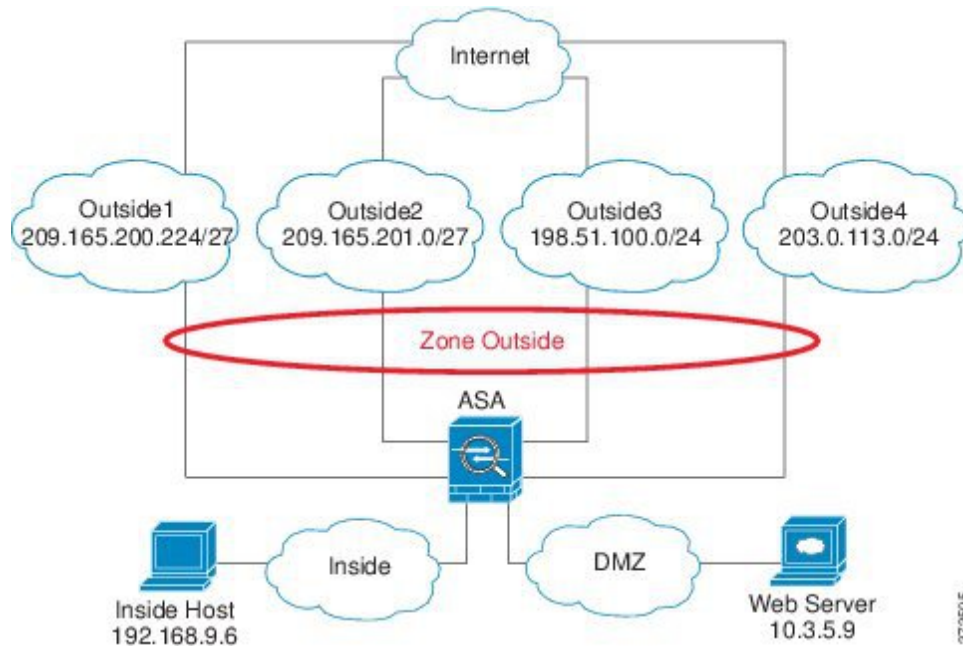
デバッグ目的で高速セキュリティ パステータブルを表示し、各ルートに関連付けられたゾーンを表示します。

show asp table routing コマンドについては次の出力を参照してください。

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1      255.255.255.255 identity
in   10.2.0.1      255.255.255.255 identity
in   10.6.6.4      255.255.255.255 identity
in   10.4.4.4      255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67    255.255.255.255 identity
in   172.0.0.0     255.255.255.0   wan-zone:outside2
in   10.85.43.0    255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0    255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0   255.255.255.0   mgmt
in   192.168.1.0   255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67     255.255.255.255 mgmt
out  172.0.0.0     255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

トラフィック ゾーンの例

次に、4つの VLAN インターフェイスを外部ゾーンに割り当てて、4つの等コストのデフォルトルートを設定する例を示します。PAT は内部インターフェイスに設定され、Web サーバはスタティック NAT を使用して DMZ インターフェイスで使用できます。



```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
```

```

no shutdown

interface gigabitethernet0/1.201
vlan 201
nameif outside3
security-level 0
ip address 198.51.100.1 255.255.255.0
zone-member outside
no shutdown

interface gigabitethernet0/1.202
vlan 202
nameif outside4
security-level 0
ip address 203.0.113.1 255.255.255.0
zone-member outside
no shutdown

interface gigabitethernet0/2.301
vlan 301
nameif inside
security-level 100
ip address 192.168.9.1 255.255.255.0
no shutdown

interface gigabitethernet0/2.302
vlan 302
nameif dmz
security-level 50
ip address 10.3.5.1 255.255.255.0
no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
host 10.3.5.9 255.255.255.255
nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
subnet 192.168.9.0 255.255.255.0
nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
dns-guard
protocol-enforcement

```

```
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

トラフィック ゾーンの履歴

機能名	プラットフォーム リリース	説明
トラフィック ゾーン	9.3(2)	インターフェイスをトラフィック ゾーンにグループ化することで、トラフィックのロードバランシング（等コストマルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングを実現できます。 （注） 名前付きゾーンにはセキュリティ ポリシーを適用できません。セキュリティポリシーはインターフェイスに基づきます。ゾーン内のインターフェイスが同じアクセスルール、NAT、およびサービスポリシーを使用して設定されている場合は、ロードバランシングおよび非対称ルーティングは正しく動作します。 zone、zone-member、show running-config zone、clear configure zone、show zone、show asp table zone、show nameif zone、show conn long、show local-host zone、show route zone、show asp table routing、clear conn zone、clear local-host zone の各コマンドが導入または変更されました。