トラフィック ゾーンの管理

1 つのトラフィック 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、ゾーン内のインターフェイスで、既存のフローのトラフィックが 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。

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るようになります。

ゾーンを使用する理由

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。

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。

関連項目

- ゾーンを使用する理由　（1 ページ）
- ECMP ルーティング　（3 ページ）
- トラフィックゾーンについて　（4 ページ）
- トラフィック ゾーンの前提条件　（6 ページ）
- トラフィック ゾーンのガイドライン　（7 ページ）
- トラフィックゾーンの設定　（8 ページ）

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 3 つの等コストのスタティックルートタ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で 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、ユーザー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。

関連項目

- ECMP ルーティング （3 ページ）
- トラフィックゾーンについて （4 ページ）
- トラフィック ゾーンの前提条件 （6 ページ）>
- トラフィック ゾーンのガイドライン （7 ページ）
- トラフィックゾーンの設定 （8 ページ）

トラフィックゾーンについて

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。必須のパラレル インターフェイス設定の詳細については、 トラフィック ゾーンの前提条件 （6 ページ）を参照してください。

トラフィック ゾ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 サービスや from-the-box サービス（以下を参照）も設定できます。

トラフィック ゾ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 ゾーンの前提条件 （6 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。

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
- BGP

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。

関連項目

- ゾーンを使用する理由 （1 ページ）
- トラフィックゾーンについて （4 ページ）
- トラフィック ゾーンの前提条件 （6 ページ）
- トラフィック ゾーンのガイドライン （7 ページ）
- トラフィックゾーンの設定 （8 ページ）

トラフィック ゾーンの前提条件

- 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る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。
  - 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。

インターフェイス PAT はサポートされていません。

（注） インターフェイス固有の NAT および PAT プールを使用すると、ASA は、元のインターフェイスに障害が発生した場合に接続を切り替えることができません。インターフェイス固有の PAT プールを使用すると、同じホストからの複数の接続が異なるインターフェイスにロードバランシングされ、異なるマッピングされた IP アドレスを使用する場合があります。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。

（注） VoIP インスペクションでは、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。順序が不正なパケットには次のような兆候が見られます。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。これらの影響を低減するために、VoIP トラフィックの負荷分散専用の IP アドレスを使用することをお勧めします。

- ECMP ゾーン機能を考慮してルーティングを設定します。

関連項目

- ゾーンを使用する理由 （1 ページ）
- ECMP ルーティング （3 ページ）
- トラフィックゾーンについて （4 ページ）
- トラフィック ゾーンのガイドライン （7 ページ）
- トラフィックゾーンの設定 （8 ページ）

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。
- 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。
- ゾーンに追加できるのは、物理インターフェイスのみです。
- 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。
- 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。
- 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。

関連項目

- ゾーンを使用する理由　（1 ページ）
- ECMP ルーティング　（3 ページ）
- トラフィックゾーンについて　（4 ページ）
- トラフィック ゾーンの前提条件　（6 ページ）
- トラフィックゾーンの設定　（8 ページ）

トラフィックゾーンの設定

1 つのトラフィック 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、ゾーン内のインターフェイスで、既存のフローのトラフィックが 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。

関連項目

- インターフェイス ロール オブジェクトについて
- ゾーンを使用する理由 （1 ページ）
- ECMP ルーティング （3 ページ）
- トラフィックゾーンについて （4 ページ）
- トラフィック ゾーンの前提条件 （6 ページ）
- トラフィック ゾーンのガイドライン （7 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーン（Zone）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーン（Zone）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [ゾーン（Zone）] テーブルの下にある [追加（Add）] ボタンをクリックして、[ゾーン（Zone）] ダイアログボックスを表示します。

ステップ 3 設定しているトラフィックゾーンに属するインターフェイスを識別するインターフェイス ロールの名前を入力し、[OK] をクリックします。インターフェイス ロール オブジェクトの詳細については、インターフェイス ロール オブジェクトについてを参照してください。

ヒント [選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイス ロールを選択するか、新しいインターフェイス ロール オブジェクトを定義します。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。