ASA 8.2.X TCP 状態バイパス機能の設定例

内容

概要

このドキュメントでは、TCP 状態バイパス機能を設定する方法について説明します。この機能によって、独立した Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス経由の着発信フローが許可されます。

前提条件

ライセンス要件

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスには少なくとも Base ライセンスが必要です。

使用するコンポーネント

このドキュメントの情報は、Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）バージョン 8.2(1) 以降に基づいています。

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。

TCP 状態バイパス

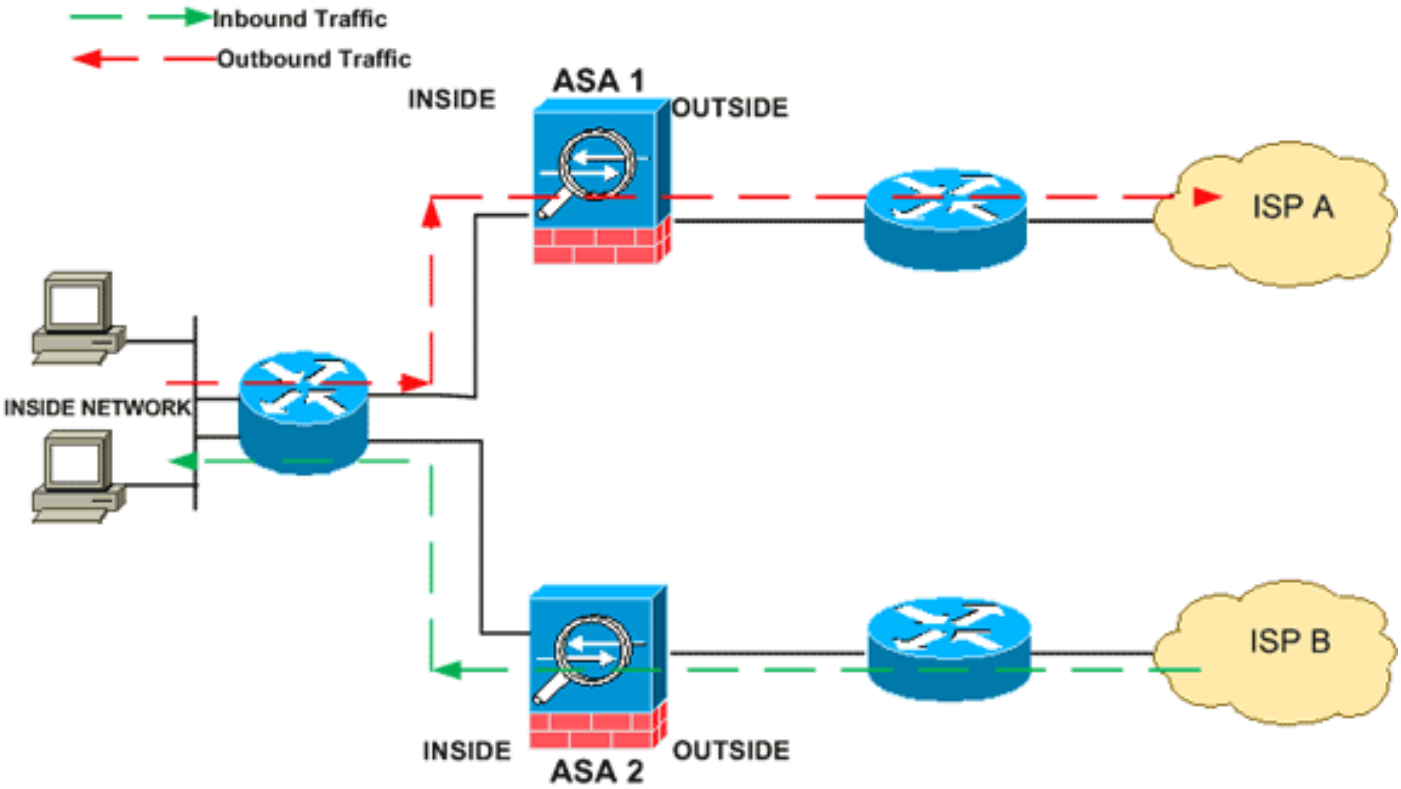
デフォルトで、Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）を通過するすべてのトラフィックは、アダプティブ セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて通過を許可されるか廃棄されます。ファイアウォールのパフォーマンスを最大限にするために、ASA は、各パケットの状態をチェック（新しい接続なのか、確立済みの接続なのかなど）し、パケットをセッション管理パス（新しい接続 SYN パケット）、高速パス（確立済みの接続）、またはコントロール プレーン パス（拡張インスペクション）のいずれかに割り当てます。

高速パス内の既存の接続に一致する TCP パケットは、セキュリティ ポリシーのすべての側面を再チェックしなくても適応型セキュリティ アプライアンスを通過できます。この機能によってパフォーマンスが最大化されます。ただし、高速パス内でセッションを確立するために使う方式（SYN パケットを使用）と高速パス内で発生するチェック（TCP シーケンス番号など）は、非対称ルーティング ソリューションの妨げになる可能性があります。非対称ルーティング ソリューションでは、1 つの接続の発信と着信のフローはどちらも同一の ASA を通過する必要があります。

たとえば、新しい接続が*ASA 1*に送信されます。SYNパケットはセッション管理パスを通過し、接続のエントリが高速パステーブルに追加されます。この接続の後に続くパケットが *ASA 1* を通る場合、パケットは高速パスのエントリと一致し、そのまま通過します。後に続くパケットが *ASA 2* に送信される場合、そこにセッション管理パスを通った SYN パケットがなかったとすると、その接続用に高速パスのエントリが存在しないので、パケットは廃棄されます。

上流のルータに非対称ルーティングを設定していて、トラフィックが 2 つの ASA 間で交互に発生する場合、特定のトラフィックに対して TCP 状態バイパスを設定できます。TCP 状態バイパスは、高速パスでセッションが確立される方法を変更し、高速パスのチェックをディセーブルにします。この機能は、UDP 接続を取り扱うのと同様に TCP トラフィックを取り扱います。指定されたネットワークに一致する非 SYN パケットが ASA に入り、高速パス エントリが存在しないときに、そのパケットは高速パスでの接続を確立するためにセッション管理パスを通過します。高速パス内に入ると、トラフィックは高速パス チェックをバイパスします。

次の図は、非対称ルーティングの例であり、ここでは、発信トラフィックが着信トラフィックとは異なる ASA を通過しています。



注：Cisco ASA 5500シリーズ適応型セキュリティアプライアンスでは、TCP状態バイパス機能はデフォルトで無効になっています。

サポート情報

このセクションでは、TCP 状態バイパス機能のサポート情報を提供しています。

- コンテキスト モード：単一および複数のコンテキスト モードでサポートされます。
- ファイアウォール モード：ルーテッド モードと透過モードでサポートされます。
- フェールオーバー：フェールオーバーをサポートします。

次の機能は、TCP 状態バイパスを使用するときにはサポートされません。

- アプリケーション検査：アプリケーション検査は、着信と発信の両方のトラフィックが同一の ASA を通過することが必要なので、アプリケーション検査は TCP 状態バイパスとともにはサポートされません。
- AAA 認証済みセッション：ユーザが 1 つの ASA を使用して認証を行うと、他の ASA 経由で戻されるトラフィックは、ユーザがその ASA を使用して認証しなかったため、拒否されます。
- TCP インターセプト、最大初期接続制限、TCP シーケンス番号ランダム化：ASA は接続の状態を追跡していないので、これらの機能は適用されません。
- TCP のノーマライズ：TCP ノーマライザはディセーブルになっています。
- SSM および SSC 機能：TCP 状態バイパスと、IPS や CSC などの SSM または SSC 上で動作するアプリケーションは、使用できません。

NAT ガイドライン：変換セッションはそれぞれの ASA 用に独立して確立されるので、TCP 状態バイパス トラフィック用に両方の ASA にスタティック NAT を必ず設定するようにします。ダイナミック NAT を使用する場合、*ASA 1* のセッション用に選択されるアドレスは、*ASA 2* のセッション用に選択されるアドレスとは異なります。

設定

このセクションでは、Cisco ASA 5500 Series Adaptive Security Appliance（ASA: 適応型セキュリティ アプライアンス）の TCP 状態バイパス機能の設定方法について説明します。

TCP 状態バイパス機能の設定

次のステップを実行して、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに TCP 状態バイパス機能を設定します。

1. **class-map class_map_name コマンドを使用してクラス マップを作成します。**クラス マップは、ステートフル ファイアウォール インスペクションをディセーブルにするトラフィックを特定するために使われます。この例で使用するクラスマップは*tcp_bypass*です。
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. **match parameter コマンドを使用して、クラス マップ内で対象のトラフィックを指定します。**モジュラ ポリシー フレームワークを使用するときは、class-map コンフィギュレーション モードで match access-list コマンドを使用してアクションを適用するトラフィックを特定するためのアクセス リストを使用します。次にこの設定の例を示します。
   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```

   tcp_bypass は、この例で使用する access-list の名前です。対象のトラフィックを指定する詳細は、「レイヤ 3/4 クラス マップによるトラフィックの特定」を参照してください。
3. **policy-map name コマンドを使用して、ポリシー マップの追加や、すでに指定されているクラス マップでアクションを実行するために設定するポリシー マップの編集（すでに存在する場合）を行います。**モジュラ ポリシー フレームワークを使用するときには、グローバル コンフィギュレーション モードで（type キーワードを指定せずに）policy-map コマンドを使用して、レイヤ 3/4 クラス マップで特定したトラフィックにアクションを割り当てます（class-map または class-map type management コマンド）。 次の例では、ポリシー マップは *tcp_bypass_policy* です。
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```

4. ポリシーマップコンフィギュレーションモードでclassコマンドを使用し、すでに作成されたクラスマップ(*tcp_bypass*)をポリシーマップ(*tcp_bypass_policy*)に割り当てます。この際、クラスマップトラフィックにアクションを割り当てることができます。この例では、クラスマップは*tcp_bypass*です。
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```

5. クラス コンフィギュレーション モードで **set connection advanced-options tcp-state-bypass コマンドを使用して、TCP 状態バイパス機能をイネーブルにします。**このコマンドはバージョン 8.2(1) から導入されました。 クラス設定モードは、次の例に示すように policy-map コンフィギュレーション モードからアクセスできます。
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
   ```

6. グローバル コンフィギュレーション モードで service-policy policymap_name [global | interface *intf*]コマンドを発行して、ポリシーマップをすべてのインターフェイスまたは対象

のインターフェイスでグローバルにアクティブ化します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。**service-policy** コマンドを使用して、1 つのインターフェイスに一連のポリシーをイネーブルにします。**global** はすべてのインターフェイスにポリシー マップを適用し、**interface** は 1 つのインターフェイスにポリシーを適用します。許可されるグローバル ポリシーは 1 つだけです。インターフェイスでは、そのインターフェイスへサービス ポリシーを適用することで、グローバル ポリシーを上書きできます。各インターフェイスに適用できるポリシー マップは 1 つだけです。

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

次に示すのは、TCP 状態バイパスのサンプル設定です。

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

!--- Configure the class map and specify the match parameter for the !--- class map to match the
interesting traffic. ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map !--- inside this policy map for the
class map. ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
!--- Use the set connection advanced-options tcp-state-bypass !--- command in order to enable
TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
!--- Use the service-policy policymap_name [ global | interface intf ] !--- command in global
configuration mode in order to activate a policy map !--- globally on all interfaces or on a
targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

確認

show conn コマンドは、アクティブな TCP と UDP の接続数を表示し、さまざまなタイプの接続についての情報を提供します。指定された接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn コマンドを使用します。**このコマンドは IPv4 と IPv6 のアドレスをサポートします。**TCP state bypass** を使用する接続の出力表示は、フラグ **b** を含んでいます。

トラブルシュート

エラー メッセージ

ASA は、TCP 状態バイパス機能がイネーブルになった後でも次のエラー メッセージを表示します。

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
```

interface_name to dest_address:no matching session
通常は有効なエコー要求がセキュリティ アプライアンス経由でまだ渡されていない ICMP エコー応答であったり、セキュリティ アプライアンスですでに確立されている TCP、UDP、または ICMP セッションに関係していない ICMP エラー メッセージであったりするステートフルな ICMP 機能によってセキュリティ チェックが追加されるため、ICMP パケットはセキュリティ アプライアンスによって廃棄されました。

TCP 状態バイパスがイネーブルになっている場合でも ASA はこのログを表示します。その理由は、この機能をディセーブルにする（つまり、接続テーブルでタイプ 3 用の ICMP 戻りエントリをチェックする）ことが不可能であるためです。ただし、TCP 状態バイパス機能は正しく動作します。

次のコマンドを使用すると、これらのメッセージが表示されるのを防止できます。

```
hostname(config)#no logging message 313004
```

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems