ASA 7.x/PIX 6.x 以降： ポートのオープンまたはブロックの設定例

目次

概要

このドキュメントでは、セキュリティ アプライアンスのさまざまなトラフィック タイプ（http または ftp など）のポートをオープンまたはブロックする方法の設定例を示します。

注: 「ポートをオープンする」と「ポートを許可する」という用語は、同じ意味を示します。 同様に、「ポートをブロッキングする」と「ポートを制限する」も同じ意味を示します。

前提条件

要件

このドキュメントでは、PIX/ASA が設定されていて適切に動作していることを前提としています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 8.2(1) で稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）

- Cisco Adaptive Security Device Manager（ASDM）バージョン 6.3(5)

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。

関連製品

この設定は、ソフトウェア バージョン 6.x 以降の Cisco 500 シリーズ PIX ファイアウォール アプライアンスにも適用できます。

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

各インターフェイスのセキュリティ レベルは、0（最低）から 100（最高）にする必要があります。 たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。 一方で、インターネットに接続する外部ネットワークはレベル 0 にしたり、DMZ などの他のネットワークは中間のレベルにしたりすることができます。 複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。

デフォルトでは、セキュリティ アプライアンスの外部インターフェイス（セキュリティ レベル 0）ではすべてのポートがブロックされ、内部インターフェイス（セキュリティ レベル 100）ではすべてのポートがオープンになります。 このように、すべての発信トラフィックは設定なしでセキュリティ アプライアンスを通過できますが、着信トラフィックはセキュリティ アプライアンスのアクセス リストとスタティック コマンドの設定によって許可できます。

注: 通常、ステートフル インスペクションが着信トラフィックと発信トラフィックの両方で有効になっている場合、低いセキュリティ ゾーンから高いセキュリティ ゾーンへのすべてのポートはブロックされ、高いセキュリティ ゾーンから低いセキュリティ ゾーンへのすべてのポートはオープンになります。

このセクションは、次に示すサブセクションで構成されます。

- ネットワーク図
- ポートをブロッキングする設定
- ポートをオープンする設定

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。

ポートをブロッキングする設定

セキュリティ アプライアンスは、拡張アクセス リストで明示的にブロックされていない限り、あらゆる発信トラフィックの通過を許可します。

アクセス リストは、1 つ以上のアクセス コントロール エントリで構成されます。 アクセス リストの種類によっては、送信元および宛先アドレス、プロトコル、ポート (TCP または UDP の場合)、ICMP のタイプ (ICMP の場合) または EtherType を指定できます。

注: ICMP などのコネクションレス型プロトコルについては、セキュリティ アプライアンスは単方向セッションを確立します。したがって、(アクセス リストを送信元インターフェイスと宛先インターフェイスに適用することで) アクセス リストで双方向の ICMP を許可するか、ICMP インスペクション エンジンをイネーブルにする必要があります。 ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

ポートをブロックするには、次の手順を実行します。通常は、内部 (高いセキュリティ ゾーン) から DMZ (低いセキュリティ ゾーン)、または DMZ から外部に対して発信されるトラフィックに適用されます。

1. 次のように、指定されたポートのトラフィックをブロックする方法でアクセス コントロール リストを作成します。
   access-list <name> extended deny <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number> access-list <name> extended permit ip any any
2. 次に、**access-group** コマンドを使用してアクティブにするアクセス リストをバインドします。
   access-group <access list name> in interface <interface name>

例：

1. **HTTP ポート トラフィックのブロック：** DMZ ネットワークに配置された IP 172.16.1.1 を持つ http (Web サーバ) へのアクセスから内部ネットワーク 10.1.1.0 をブロックするには、次のように ACL を作成します。`ciscoasa(config)#`**access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80** `ciscoasa(config)#`**access-list 100 extended permit ip any any** `ciscoasa(config)#`**access-group 100 in interface inside** **注:** ポートのブロッキングを解除するには、**no** に続けて access list コマンドを使用します。
2. **FTP ポート トラフィックのブロック：** DMZ ネットワークに配置された IP 172.16.1.2 を持つ FTP (ファイル サーバ) へのアクセスから内部ネットワーク 10.1.1.0 をブロックするには、次のように ACL を作成します。`ciscoasa(config)#`**access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21** `ciscoasa(config)#`**access-list 100 extended permit ip any any** `ciscoasa(config)#`**access-group 100 in interface inside**

注: ポートの割り当てに関する詳細については、「IANA のポート」を参照してください。

このセクションでは、ASDM 経由で設定を行う詳細な手順を紹介しています。

1. [Configuration] > [Firewall] > [Access Rules] に移動します。 アクセス リストを作成するために、[Add Access Rule] をクリックします。
2. このアクセス ルールが関連付けられるインターフェイスとともに、アクセス ルールの送信元と宛先およびアクションを定義します。 詳細を選択し、ブロックする特定のポートを選択します。
3. 使用できるポートのリストから [http] を選択し、[OK] をクリックして [Add Access Rule] ウィンドウに戻ります。
4. [OK] をクリックして、アクセス ルールの設定を完了します。
5. 同じアクセス リストにアクセス ルールを追加するには、[Insert After] をクリックします。

6. 「any」から「any」へのトラフィックを許可し、「暗黙拒否」を回避します。 次に、[OK] をクリックして、このアクセス ルールの追加を完了します。
7. 設定したアクセス リストは、[Access Rules] タブに表示されます。 [Apply] をクリックして、セキュリティ アプライアンスに設定を送信します。ASDM から送信された設定の結果は、ASA のコマンドライン インターフェイス (CLI) の次のコマンド セットになります。
   ```
   access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
   access-list inside_access_in extended permit ip any any
   access-group inside_access_in in interface inside
   ```
   これらの手順によって、例 1 は ASDM を介して 10.1.1.0 のネットワークの Web サーバ 172.16.1.1 へのアクセスをブロックすることによって実行されました。 同様に、10.1.1.0 のネットワーク全体の FTP サーバ 172.16.1.2 へのアクセスをブロックすることによって例 2 を実現できます。 唯一の違いは、ポートの選択です。**注:** 例 2 のアクセス ルールの設定は、新しい設定とみなされます。
8. FTP トラフィックをブロックするアクセス ルールを定義し、[Details] タブをクリックして宛先ポートを選択します。
9. [ftp] ポートを選択し、[OK] をクリックして [Add Access Rule] ウィンドウに戻ります。
10. [OK] をクリックして、アクセス ルールの設定を完了します。
11. その他のトラフィックを許可する別のアクセス ルールを追加します。 そうしないと、暗黙拒否ルールによってインターフェイス上のすべてのトラフィックがブロックされます。
12. 完成したアクセス リストの設定は、[Access Rules] タブの下に次のように表示されます。
13. [Apply] をクリックして設定を ASA に送信します。 同等の CLI 設定は次のようになります。
    ```
    access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
    access-list inside_access_in extended permit ip any any
    access-group inside_access_in in interface inside
    ```

ポートをオープンする設定

セキュリティ アプライアンスは、拡張アクセス リストで明示的に許可されていないかぎり、どのような着信トラフィックの通過も許可しません。

外部ホストから内部ホストにアクセスできるようにする場合は、外部インターフェイス上で着信アクセス リストを適用できます。 内部ホストの変換後アドレスは外部ネットワーク上で使用できるアドレスであるため、変換後アドレスをアクセス リストで指定する必要があります 低いセキュリティ ゾーンから高いセキュリティ ゾーンに対してポートをオープンするには、次の手順を実行します。 たとえば、外部 (低いセキュリティ ゾーン) から内部インターフェイス (高いセキュリティ ゾーン)、または DMZ から内部インターフェイスへのトラフィックを許可します。

1. スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。 マッピングされたこのアドレスはインターネット上でホストされるアドレスで、サーバの実際のアドレスを知らなくても DMZ 上のアプリケーション サーバに対するアクセスに使用できるアドレスです。
   static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] | access-list access_list_name | interface} 詳細については、『PIX/ASA のコマンド リファレンス』の「スタティック NAT」セクションを参照してください。
2. 1 つの ACL を作成して特定のポートのトラフィックを許可します。
   access-list <name> extended permit <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number>
3. 次に、**access-group** コマンドを使用してアクティブにするアクセス リストをバインドします。
   access-group <access-list name> in interface <interface name>

例：

1. **SMTP ポート トラフィックのオープン：** ポート **tcp 25** をオープンし、外部（インターネット）からのホストが DMZ ネットワークに配置されたメール サーバにアクセスできるようにします。**Static** コマンドは、外部アドレスの 192.168.5.3 を実際の DMZ アドレス 172.16.1.3 にマッピングします。`ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.3 eq 25 ciscoasa(config)#access-group 100 in interface outside`
2. **HTTPS ポート トラフィックのオープン：** ポート **tcp 443** をオープンし、外部（インターネット）からのホストが DMZ ネットワークに配置された Web サーバ（セキュア）にアクセスできるようにします。`ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.5 eq 443 ciscoasa(config)#access-group 100 in interface outside`
3. **DNS トラフィックの許可：** ポート **udp 53** をオープンし、外部（インターネット）からのホストが DMZ ネットワークに配置された DNS サーバ（セキュア）にアクセスできるようにします。`ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit udp any host 192.168.5.4 eq 53 ciscoasa(config)#access-group 100 in interface outside`

注: ポートの割り当てに関する詳細については、「IANA のポート」を参照してください。

ASDM 経由の設定

このセクションでは、前述したタスクを ASDM で実行するための詳細な手順を紹介しています。

1. 192.168.5.3 サーバへの smtp トラフィックを許可するアクセス ルールを作成します。
2. アクセス ルールの送信元と宛先、このルールがバインドされるインターフェイスを定義します。 また、[Action] に [Permit] を定義します。
3. ポートに [SMTP] を選択し、[OK] をクリックします。
4. [OK] をクリックして、アクセス ルールの設定を完了します。
5. 172.16.1.3 を 192.168.5.3 に変換するために、スタティック NAT を設定します。[Configuration] > [Firewall] > [NAT Rules] > [Add Static NAT Rule] に移動し、スタティック NAT エントリを追加します。関連付けられているインターフェイスとともに変換前のソース アドレスと変換後の IP アドレスを選択し、[OK] をクリックしてスタティック NAT のルールの設定を完了します。このイメージは、「例」セクションに記載されている 3 つのスタティック ルールすべてを図示しています。このイメージは、「例」セクションに記載されている 3 つのアクセス ルールすべてを図示しています。

確認

次に示すように、特定の show コマンドで確認できます。

- **show xlate**：現在の変換情報の表示
- **show access-list**：アクセス ポリシーのヒット カウンタの表示
- **show logging**：バッファ内のログの表示

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。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- PIX/ASA 7.x： インターフェイス間通信の有効化および無効化
- nat、global、static access-list PIX 7.0
- PIX での nat、global、static、conduit、および access-list の各コマンドとポート リダイレクション (フォワーディング) の使用方法
- PIX/ASA 7.x： FTP/TFTP サービスの有効化の設定例
- PIX/ASA 7.x： VoIP (SIP、MGCP、H323、SCCP) サービス有効化の設定例
- PIX/ASA 7.x： DMZ でのメール サーバ アクセスの設定例
- テクニカルサポートとドキュメント - Cisco Systems