ASA/PIX/IOS のルータの IPS での回避/ブロックの設定例

目次

はじめに

このドキュメントでは、Cisco IPSを使用してPIX/ASA/Cisco IOSルータでシャニングを設定する方法について説明します。センサーのブロッキングアプリケーションであるARCは、ルータ、Cisco 5000 RSMおよびCatalyst 6500シリーズスイッチ、PIX Firewall、FWSM、およびASAのブロックを開始および停止します。ARCは、悪意のあるIPアドレスのブロックまたは回避を管理対象デバイスに発行します。ARCは、センサーが管理するすべてのデバイスに同じブロックを送信します。プライマリブロッキングセンサーが設定されている場合、ブロックはこのデバイスに転送され、このデバイスから発行されます。ARC は、ブロック時間をモニタし、時間の経過後にブロックを削除します。

IPS 5.1を使用する場合は、マルチコンテキストモードでファイアウォールにシャニングする際に特別な注意が必要です。これは、shun要求とともにVLAN情報が送信されないためです。

> **注**：マルチコンテキストFWSMの管理コンテキストでは、ブロッキングはサポートされません。

ブロックには、次の3つのタイプがあります。

- ホストブロック：特定のIPアドレスからのすべてのトラフィックをブロックします。
- 接続ブロック：特定の送信元IPアドレスから特定の宛先IPアドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元IPアドレスから別の宛先IPアドレスまたは宛先ポートへの複数の接続ブロックは、ブロックを接続ブロックからホストブロックに自動的に切り替えます。**注**：接続ブロックは、セキュリティアプライアンスではサポートされていません。セキュリティアプライアンスは、オプションのポートおよびプロトコル情報を持つホストブロックのみをサポートします。

- ネットワークブロック：特定のネットワークからのすべてのトラフィックをブロックします。ホストおよび接続ブロックは、シグニチャがトリガーされたときに手動または自動で開始できます。ネットワークブロックは手動でのみ開始できます。

自動ブロックの場合、シグニチャがトリガーされたときにSensorAppがブロック要求をARCに送信するように、特定のシグニチャのイベントアクションとして[Request Block Host or Request Block Connection]を選択する必要があります。ARCはSensorAppからブロック要求を受信すると、デバイス設定を更新してホストまたは接続をブロックします。Request Block HostまたはRequest Block Connectionイベントアクションをシグニチャに追加する手順の詳細は、『シグニチャへのアクションの割り当て』の5-22ページを参照してください。特定のリスクレーティングのアラームにRequest Block HostまたはRequest Block Connectionイベントアクションを追加するオーバーライドの設定手順の詳細は、『イベントアクションオーバーライドの設定』の7-15ページを参照してください。

CiscoルータおよびCatalyst 6500シリーズスイッチでは、ARCはACLまたはVACLを適用してブロックを作成します。ACLおよびVACLは、トラフィックを許可または拒否するために、方向およびVLANを含むインターフェイスにそれぞれフィルタを適用します。.PIX Firewall、FWSM、およびASAはACLまたはVACLを使用しません。組み込みの**shun**コマンドと**no shun**コマンドを使用します。

ARCの設定には、次の情報が必要です。

- デバイスにAAAが設定されている場合、ログインユーザID
- ログインパスワード
- イネーブルパスワード。ユーザがイネーブルアクセス権を持っている場合は不要
- 管理対象のインターフェイス（ethernet0、vlan100など）
- 作成されたACLまたはVACLの先頭（Pre-Block ACLまたはVACL）または末尾（Post-Block ACLまたはVACL）に適用する既存のACLまたはVACL情報。PIX Firewall、FWSM、またはASAではブロックにACLまたはVACLを使用しないため、この設定は適用されません。
- TelnetまたはSSHを使用してデバイスと通信するかどうか
- ブロックしないIPアドレス（ホストまたはホストの範囲）
- ブロックの長さを指定する

前提条件

要件

ブロッキングまたはレート制限のためにARCを設定する前に、次のタスクを実行する必要があります。

- ネットワークトポロジを分析して、どのデバイスがどのセンサーによってブロックされるべきか、どのアドレスがブロックされるべきかを理解します。
- 各デバイスへのログインに必要なユーザ名、デバイスパスワード、イネーブルパスワード、および接続タイプ（TelnetまたはSSH）を収集します。
- デバイスのインターフェイス名を知っている。
- 必要に応じて、ブロック前ACLまたはVACLの名前とブロック後ACLまたはVACLの名前を確認します。
- ブロックする必要があるインターフェイスとブロックしないインターフェイス、およびブロックする方向（インまたはアウト）を理解します。

使用するコンポーネント

このドキュメントの情報は、Cisco Intrusion Prevention System 5.1以降に基づくものです。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

> **注**：デフォルトでは、ARCは250個のブロックエントリの制限に設定されています。ARCがサポートするブロッキングデバイスのリストの詳細は、『サポートされるデバイス』を参照してください。

表記法

ドキュメント表記の詳細については、『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。

背景説明

ブロックとレート制限を有効にするために必要な基本設定を構成するには、[Blocking]ページを使用します。

ARCは、管理対象デバイスのブロックおよびレート制限アクションを制御します。

ブロックされないホストとネットワークを特定するには、センサーを調整する必要があります。信頼できるデバイスのトラフィックがシグニチャを起動する可能性があります。このシグニチャが攻撃者をブロックするように設定されている場合、正当なネットワークトラフィックが影響を受ける可能性があります。このシナリオを回避するために、デバイスのIPアドレスをNever Blockリストにリストできます。

Never Blockエントリで指定されたネットマスクは、Never Blockアドレスに適用されます。ネットマスクを指定しない場合は、デフォルトの/32マスクが適用されます。

> **注**：デフォルトでは、センサーとブロッキングデバイス間の通信に干渉するため、センサーは自身のIPアドレスに対してブロックを発行できません。ただし、このオプションはユーザが設定できます。

ブロッキングデバイスを管理するようにARCを設定したら、ブロッキングデバイスのシャンスと、ブロッキングに使用されるACL/VACLを手動で変更しないでください。これにより、ARCサービスが中断し、将来ブロックが発行されない可能性があります。

> **注**：デフォルトでは、ブロックのみがCisco IOSデバイスでサポートされています。レート制限またはブロックおよびレート制限を選択すると、ブロッキングデフォルトを上書きできます。

ブロックを発行または変更するには、IPSユーザに管理者ロールまたはオペレータロールが必要です。

Ciscoルータを管理するためのセンサーの設定

このセクションでは、Ciscoルータを管理するためのセンサーの設定方法について説明します。次のトピックが含まれています。

- ユーザプロファイルの設定
- ルータとACL
- CLIを使用したCiscoルータの設定

ユーザプロファイルの設定

センサーは、**user-profiles** *profile_name*コマンドを使用して他のデバイスを管理し、ユーザプロファイルを設定します。ユーザプロファイルには、ユーザID、パスワード、およびイネーブルパスワード情報が含まれています。たとえば、すべてのルータが同じパスワードとユーザ名を共有している場合は、1つのユーザプロファイルの下に配置できます。

> **注**：ブロックするデバイスを設定する前に、ユーザプロファイルを作成する必要があります。

ユーザプロファイルを設定するには、次の手順を実行します。

1. 管理者権限を持つアカウントでCLIにログインします。
2. ネットワークアクセスモードに入ります。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. ユーザプロファイル名を作成します。
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```
4. そのユーザプロファイルのユーザ名を入力します。
   ```
   sensor(config-net-use)#username username
   ```
5. ユーザのパスワードを指定します。
   ```
   sensor(config-net-use)# password
   Enter password[]: ********
   Re-enter password ********
   ```
6. ユーザのイネーブルパスワードを指定します。
   ```
   sensor(config-net-use)# enable-password
   Enter enable-password[]: ********
   Re-enter enable-password ********
   ```
7. 設定を確認します。
   ```
   sensor(config-net-use)#show settings
      profile-name: PROFILE1
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: jsmith default:
      -----------------------------------------------
   ```

```
sensor(config-net-use)#
```

8. ネットワークアクセスサブモードを終了します。

```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```

9. 変更を適用する場合は Enter キーを押し、変更を廃棄する場合は [no] を入力します。

ルータとACL

ACLを使用するブロッキングデバイスでARCを設定すると、ACLは次のように構成されます。

1. センサーのIPアドレスを持つ許可ライン、または指定されている場合はセンサーのNATアドレス**注**：センサーのブロックを許可すると、この行はACLに表示されません。
2. プレブロックACL（指定されている場合）:このACLはデバイスにすでに存在している必要があります。**注**：ARCは事前設定されたACLの行を読み取り、これらの行をブロックACLの先頭にコピーします。
3. すべてのアクティブブロック
4. **Post-Block ACL**または**permit ip any any**:**ポストブロックACL**（指定されている場合）:このACLはデバイスにすでに存在している必要があります。**注**：ARCはACL内の行を読み取り、ACLの最後にコピーします。**注**：一致しないパケットをすべて許可する場合は、ACLの最後の行がpermit ip any anyであることを確認します。**permit ip any any**（ポストブロックACLが指定されている場合は使用されません）

注：ARCが作成するACLは、ユーザや他のシステムによって変更されることはありません。これらのACLは一時的なものであり、新しいACLは常にセンサーによって作成されます。Pre-Block ACLとPost-Block ACLに対して行える変更は他にありません。

ブロック前ACLまたはブロック後ACLを変更する必要がある場合は、次の手順を実行します。

1. センサーのブロッキングを無効にします。
2. デバイスの設定を変更します。
3. センサーのブロッキングを再度有効にします。

ブロッキングが再度有効になると、センサーは新しいデバイス設定を読み取ります。

注：1つのセンサーで複数のデバイスを管理できますが、複数のセンサーで1つのデバイスを管理することはできません。複数のセンサーから発行されたブロックが単一のブロッキングデバイス用である場合、プライマリブロッキングセンサーを設計に組み込む必要があります。プライマリブロッキングセンサーは、複数のセンサーからブロッキング要求を受信し、ブロッキングデバイスにすべてのブロッキング要求を発行します。

プレブロックACLとポストブロックACLは、ルータ設定で作成して保存します。これらのACLは、名前付きまたは番号付きの拡張IP ACLである必要があります。ACLの作成方法については、ルータのマニュアルを参照してください。

注：プレブロックおよびポストブロックACLは、レート制限には適用されません。

ACLはトップダウンで評価され、最初の一致アクションが実行されます。ブロック前ACLには、ブロックによって発生した拒否よりも優先される許可が含まれている場合があります。

ブロック後ACLは、ブロック前ACLまたはブロックで処理されない条件を考慮するために使用されます。インターフェイスに既存のACLがあり、ブロックが発行される方向にある場合、そのACLをポストブロックACLとして使用できます。ポストブロックACLがない場合、センサーは新しいACLの最後にpermit ip any anyを挿入します。

センサーが起動すると、2つのACLの内容が読み取られます。次のエントリを持つ3番目のACLを作成します。

- センサーのIPアドレスの許可行
- ブロック前ACLのすべての設定行のコピー
- センサーによってブロックされている各アドレスの拒否行
- ポストブロックACLのすべての設定行のコピー

センサーは、指定したインターフェイスと方向に新しいACLを適用します。

> **注**：新しいブロックACLがルータのインターフェイスに特定の方向で適用されると、その方向のインターフェイス上にある既存のACLが置き換えられます。

CLIを使用したCiscoルータの設定

ブロッキングとレート制限を実行するようにCiscoルータを管理するセンサーを設定するには、次の手順を実行します。

1. 管理者権限を持つアカウントでCLIにログインします。
2. ネットワークアクセスサブモードに入ります。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. ARCによって制御されるルータのIPアドレスを指定します。
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. ユーザプロファイルの設定時に作成した論理デバイス名を入力します。
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   注：ARCは入力した内容をすべて受け入れます。ユーザプロファイルが存在するかどうかを確認しません。
5. センサーへのアクセスに使用する方法を指定します。
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```
   指定しない場合は、SSH 3DESが使用されます。**注**：DESまたは3DESを使用する場合は、**ssh host-key ip_address**コマンドを使用して、デバイスからSSHキーを受け入れる必要があります。
6. センサーのNATアドレスを指定します。
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   注：これにより、ACLの1行目のIPアドレスがセンサーのアドレスからNATアドレスに変更されます。NATアドレスは、センサーとブロッキングデバイスの間に配置された、中間デバイスによって変換されるセンサーアドレスNAT後です。
7. ルータがブロッキング、レート制限、またはその両方を実行するかどうかを指定します。**注**：デフォルトはブロッキングです。ルータにブロッキングのみを実行させる場合は、応答機能を設定する必要はありません。レート制限のみ
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

ブロッキングとレート制限の両方
```
sensor(config-net-rou)#response-capabilities block|rate-limit
```

8. インターフェイス名と方向を指定します。
```
sensor(config-net-rou)#block-interfaces interface_name {in | out}
```

注：インターフェイスの名前は、**interface**コマンドの後にルータが使用した場合に認識する省略形である必要があります。

9. （オプション）プレACL名を追加します（ブロッキングのみ）。
```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```
10. （オプション）ポストACL名を追加します（ブロッキングのみ）。
```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```
11. 設定を確認します。
```
sensor(config-net-rou-blo)#exit

sensor(config-net-rou)#show settings

   ip-address: 10.89.127.97
   ------------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      ------------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         ------------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      response-capabilities: block|rate-limit default: block
   ------------------------------------------------
sensor(config-net-rou)#
```
12. ネットワークアクセスサブモードを終了します。
```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
13. 変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は [no] を入力します。

Ciscoファイアウォールを管理するためのセンサーの設定

Ciscoファイアウォールを管理するようにセンサーを設定するには、次の手順を実行します。

1. 管理者権限を持つアカウントでCLIにログインします。
2. ネットワークアクセスサブモードに入ります。
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. ARCによって制御されるファイアウォールのIPアドレスを指定します。
```
sensor(config-net)#firewall-devices ip_address
```
4. ユーザプロファイルの設定時に作成したユーザプロファイル名を入力します。
```
sensor(config-net-fir)#profile-name user_profile_name
```
注：ARCは入力するものすべてを受け入れます。論理デバイスが存在するかどうかを確認しません。

5. センサーへのアクセスに使用する方法を指定します。
   ```
   sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
   ```
   指定しない場合は、SSH 3DESが使用されます。**注：**DESまたは3DESを使用する場合は、**ssh host-key ip_address**コマンドを使用してキーを受け入れる必要があります。そうしないと、ARCがデバイスに接続できません。
6. センサーのNATアドレスを指定します。
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   注：これにより、ACLの1行目のIPアドレスがセンサーのIPアドレスからNATアドレスに変更されます。NATアドレスは、センサーとブロッキングデバイスの間に配置された、中間デバイスによって変換されるセンサーアドレスNAT後です。
7. ネットワークアクセスサブモードを終了します。
   ```
   sensor(config-net-fir)#exit
   sensor(config-net)#exit
   sensor(config)#exit
   Apply Changes:?[yes]:
   ```
8. 変更を適用する場合は**Enter** キーを押し、変更を廃棄する場合は **[no] を入力します。**

PIX/ASAでのSHUNを使用したブロック

shunコマンドを発行すると、攻撃ホストからの接続がブロックされます。コマンドの値に一致するパケットは、ブロック機能が削除されるまで廃棄され、ログに記録されます。**shun**は、指定されたホストアドレスとの接続が現在アクティブであるかどうかに関係なく適用されます。

宛先アドレス、送信元ポートと宛先ポート、およびプロトコルを指定すると、それらのパラメータに一致する接続にshunを絞り込みます。送信元IPアドレスごとに1つの**shun**コマンドしか使用できません。

shunコマンドは攻撃を動的にブロックするために使用されるため、セキュリティアプライアンスの設定には表示されません。

インターフェイスが削除されると、そのインターフェイスに接続されているすべての分路も削除されます。

この例は、問題のホスト(10.1.1.27)がTCPに対して攻撃対象(10.2.2.89)と接続していることを示しています。セキュリティアプライアンスの接続テーブルの接続は、次のように表示されます。

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

攻撃ホストからの接続をブロックするには、特権EXECモードで**shun**コマンドを使用します。**shun**コマンドを次のオプションで適用します。

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

このコマンドは、セキュリティアプライアンスの接続テーブルから接続を削除し、10.1.1.27:555(TCP)から10.2.2.89:666(TCP)へのパケットがセキュリティアプライアンスを通過することを防止します。

関連情報

- Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータを管理するためのセンサーの設定
- テクニカル サポートとドキュメント – Cisco Systems