RV34xシリーズルータのACLのベストプラクティス

目的

この記事の目的は、RV34xシリーズルータでアクセスコントロールリスト(ACL)を作成するためのベストプラクティスを説明することです。

該当するデバイス |ファームウェアのバージョン

- RV340 | 1.0.03.20 **（最新版をダウンロード）**
- RV340W | 1.0.03.20 **（最新版をダウンロード）**
- RV345 | 1.0.03.20 **（最新版をダウンロード）**
- RV345P | 1.0.03.20 **（最新版をダウンロード）**

概要

ネットワークをより細かく制御したいですか。ネットワークのセキュリティを維持するために、追加の手順を実行しますか？その場合、アクセスコントロールリスト(ACL)が必要な内容になる可能性があります。

ACLは、ネットワークトラフィックプロファイルを集合的に定義する1つ以上のアクセスコントロールエントリ(ACE)で構成されます。このプロファイルは、トラフィックフィルタリング、プライオリティ、カスタムキューイングなどのシスコソフトウェア機能によって参照できます。各ACLは、送信元アドレス、宛先アドレス、プロトコル、プロトコル固有のパラメータなどの基準に基づいて、アクション要素（許可または拒否）とフィルタ要素を含む。

入力した基準に基づいて、特定のトラフィックがネットワークに出入りするのを制御できます。ルータはパケットを受信すると、パケットを調べて、アクセスリストに基づいてパケットを転送するかドロップするかを判断します。

このセキュリティレベルの実装は、特定のネットワークシナリオとセキュリティニーズを考慮したさまざまなユースケースに基づいています。

ルータは、ルータの設定に基づいて自動的にアクセスリストを作成する可能性があることに注意してください。この場合、ルータの設定を変更しない限り消去できないアクセスリストが表示されることがあります。

アクセスリストを使用する理由

- ほとんどの場合、ACLを使用して、ネットワークにアクセスするための基本的なセキュリティレベルを提供します。たとえば、ACLを設定しない場合、デフォルトでは、ルータを通過するすべてのパケットがネットワークのすべての部分に許可されます。
- ACLは、1つのホスト、IPアドレスまたはネットワークの範囲を許可し、別のホスト、

IPアドレスまたはネットワークの範囲が同じエリア（ホストまたはネットワーク）にアクセスするのを防止できます。
- ACLを使用すると、ルータインターフェイスで転送またはブロックするトラフィックのタイプを決定できます。たとえば、セキュアシェル(SSH)ファイル転送プロトコル(SFTP)トラフィックを許可すると同時に、すべてのセッション開始プロトコル(SIP)トラフィックをブロックできます。

アクセスリストを使用する場合

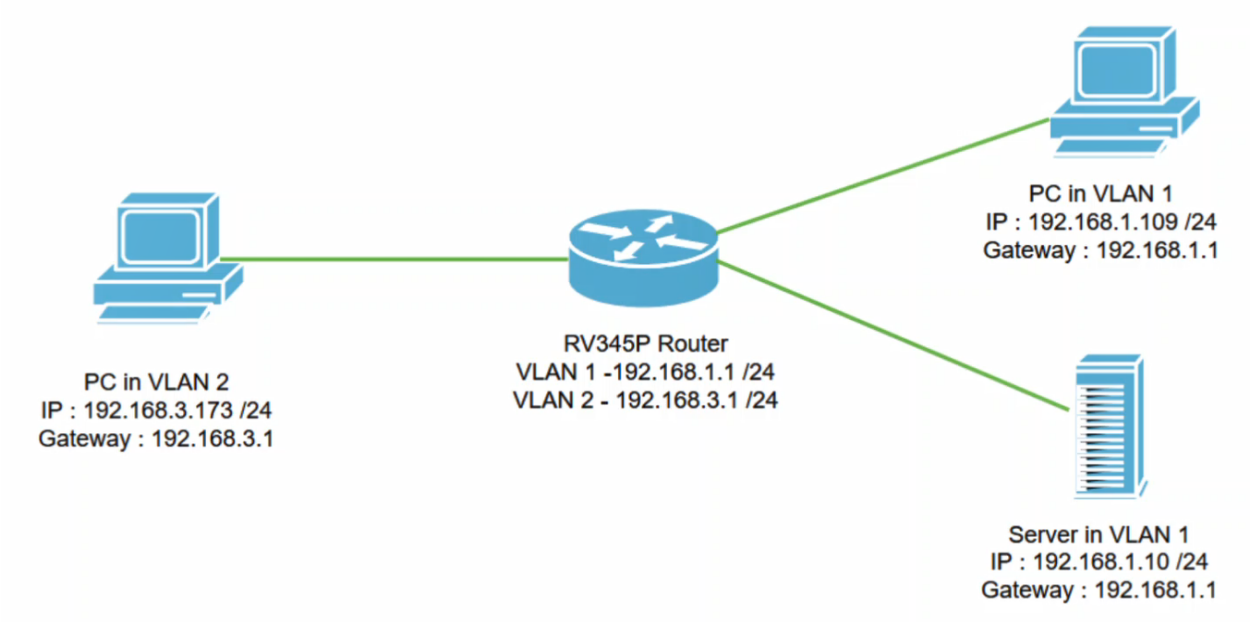
- 内部ネットワークとインターネットなどの外部ネットワークの間に位置するルータにACLを設定する必要があります。
- ACLを使用して、内部ネットワークの特定の部分に出入りするトラフィックを制御できます。
- 着信トラフィックまたは発信トラフィック、または両方をインターフェイスでフィルタリングする必要がある場合。
- トラフィックを制御するには、プロトコルごとにACLを定義する必要があります。

アクセスリストを使用して基本的なセキュリティを設定するためのベストプラクティス

- 他のすべてを拒否するプロトコル、ポート、およびIPアドレスだけを許可するACLを実装します。
- 宛先アドレスと送信元アドレスが同じであると主張する着信パケットをブロックします（ルータ自体へのランド攻撃）。
- 内部（信頼できる）SyslogホストへのACLのロギング機能をオンにします。
- ルータで簡易ネットワーク管理プロトコル(SNMP)を使用する場合は、SNMP ACLと複雑なSNMPコミュニティストリングを設定する必要があります。
- 内部アドレスだけが内部インターフェイスからルータに入ることを許可し、内部アドレス宛てのトラフィックだけが外部（外部インターフェイス）からルータに入ることを許可します。
- マルチキャストを使用しない場合はブロックします。
- 一部のインターネット制御メッセージプロトコル(ICMP)メッセージタイプ（リダイレクト、エコー）をブロックします。
- ACLを入力する順序を常に考慮してください。たとえば、ルータがパケットを転送するかブロックするかを決定する際、ACLが作成された順序で各ACLステートメントに対してパケットをテストします。

Cisco RV34xシリーズルータでのアクセスリストの実装

ネットワークトポロジの例



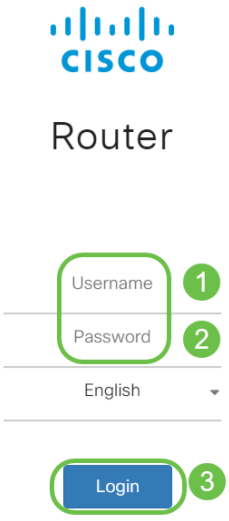
シナリオ例

このシナリオでは、RV345Pルータと2つの異なるVLANインターフェイスがあるネットワークダイアグラムを複製します。VLAN 1とVLAN2にPCがあり、VLAN 1にもサーバがあります。VLAN間ルーティングが有効になっているため、VLAN 1とVLAN 2ユーザは互いに通信できます。次に、アクセスルールを適用して、VLAN 2ユーザからVLAN 1内のこのサーバへの通信を制限します。

設定例

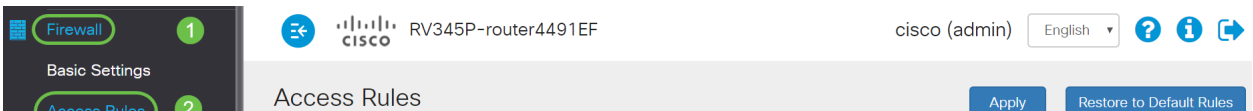
手順 1

設定したクレデンシャルを使用して、ルータのWebユーザインターフェイス(UI)にログインします。



手順 2

ACLを設定するには、[ファイアウォール] > **[アクセスルール]に移動**し、プラス記号のアイコン**をクリック**して新しいルールを追加します。



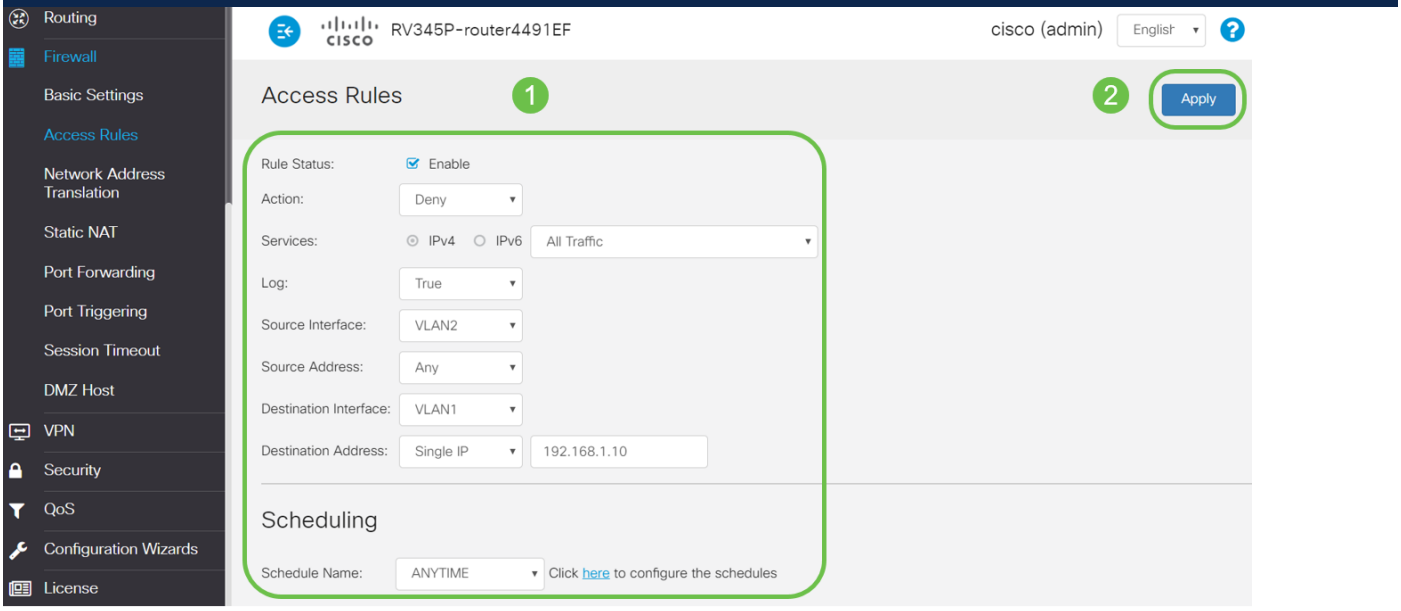
手順 3

アクセス・ルールのパラメータを構成します。ACLを適用してサーバを制限する(IPv4:192.168.1.10/24)にアクセスします。このシナリオでは、パラメータは次のようになります。

- *ルールステータス：Enable*
- *Action:拒否*
- *サービス：all traffic*
- *ログ:正しい*
- *送信元インターフェイス:VLAN2*
- *発信元アドレス：[Any]*
- *宛先インターフェイス：VLAN1*
- *宛先アドレス:シングルIP 192.168.1.10*
- *スケジュール名：いつでも*

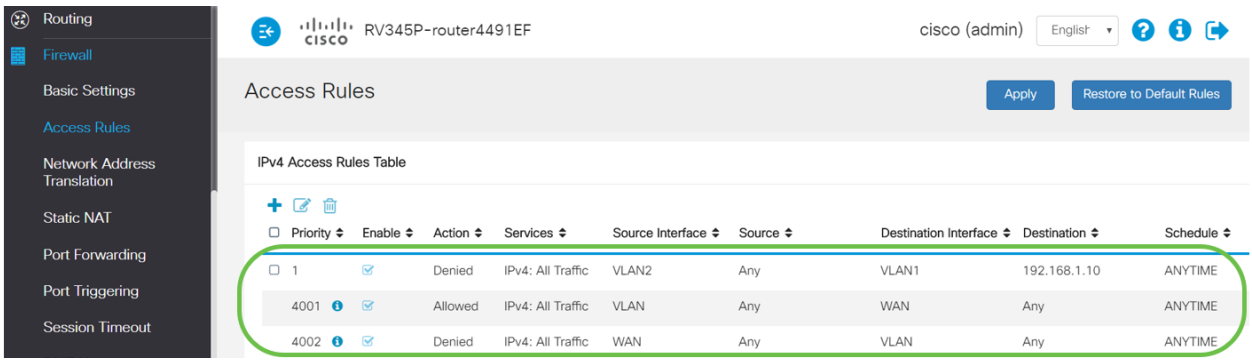
[Apply] をクリックします。

この例では、VLAN2からサーバへの任意のデバイスからのアクセスを拒否し、VLAN1の他のデバイスへのアクセスを許可しました。ニーズは異なる場合があります。



手順 4

アクセスルールのリストは次のように表示されます。



確認

サービスを確認するには、コマンドプロンプトを開きます。Windowsプラットフォームでは、Windowsボタンをクリックし、コンピュータの左下の検索ボックスに**cmdと入力して**、メニューからコマンドプロンプ**トを選択**します。

次のコマンドを入力します。

- VLAN2のPC(192.168.3.173)で、サーバ(IP:192.168.1.10) をキャプチャします。Request timed out通知が表示され、*通信が許可*されていないことを示します。
- VLAN2のPC(192.168.3.173)で、VLAN1の他のPC(192.168.1.109)にpingを実行します。正常な応答が得られます。

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

結論

Cisco RV34xシリーズルータでアクセスルールを設定するために必要な手順を確認しました。これで、ニーズに合ったアクセスルールをネットワークに作成するために適用できます。