

RV160およびRV260シリーズルータのアクセス ルールの設定

目的

ルータは外部ネットワークからデータを受信する責任があり、ローカルネットワークセキュリティに関しては最初の防衛線となります。ルータでアクセスルールを有効にすると、IPアドレスやポート番号などの特定のパラメータに基づいてパケットをフィルタリングできます。このドキュメントでは、ネットワークに入るパケットをより適切に制御するためのアクセスルールの設定方法について説明します。このドキュメントでは、アクセスルールを使用して最高のセキュリティを実現するためのベストプラクティスについても説明します。

該当するデバイス

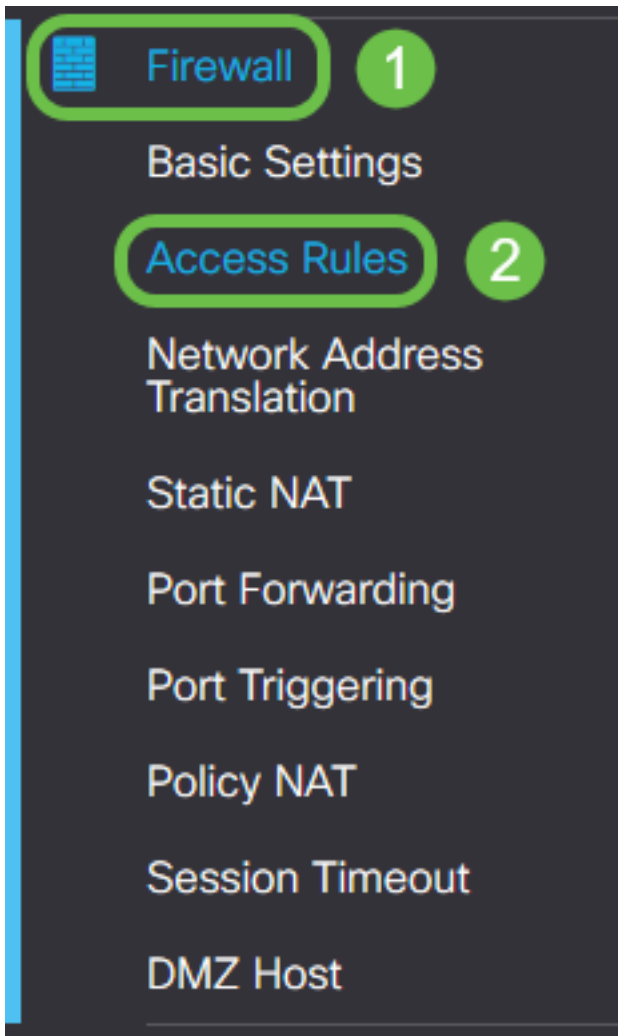
- RV160x
- RV260x

[Software Version]

- 1.0.00.13

アクセスルールの設定

ステップ1：構成ユーティリティの左側のナビゲーション・ペインで、**[Firewall]** > **[Access Rules]** を選択します。



[Access Rules]ページが表示されます。このページには、IPv4とIPv6のアクセスルールとその属性のリストを含むテーブルがあります。ここから、新しいアクセスルールを追加したり、既存のルールを編集したり、既存のルールを削除したりできます。

アクセスルールの追加/編集

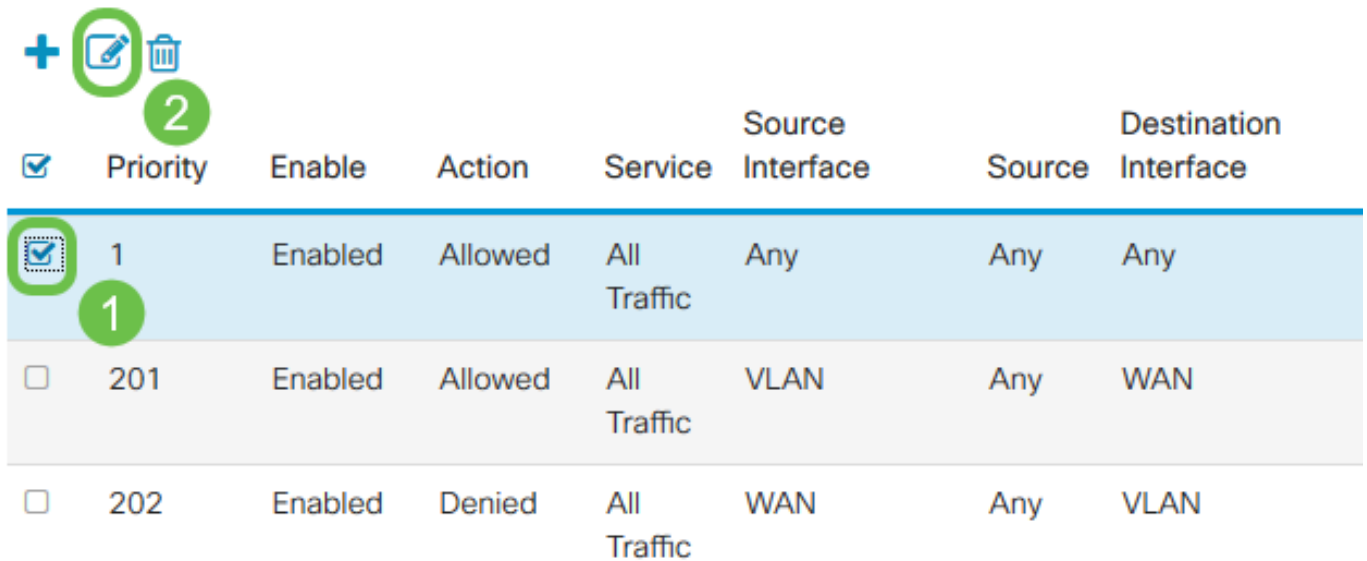
ステップ2：新しいアクセスルールを追加するには、ルールを適用するプロトコルに応じて、[IPv4 Access Rules]テーブルまたは[IPv6 Access Rules]テーブルに追加する青いアイコンをクリックします。この例では、IPv4が使用されます。

IPv4 Access Rules Table



既存のエントリを編集するには、変更するアクセスルールの横にあるチェックボックスをオンにします。次に、対応するテーブルの上部にある青い編集アイコンを選択します。一度に選択できる規則は1つだけです。

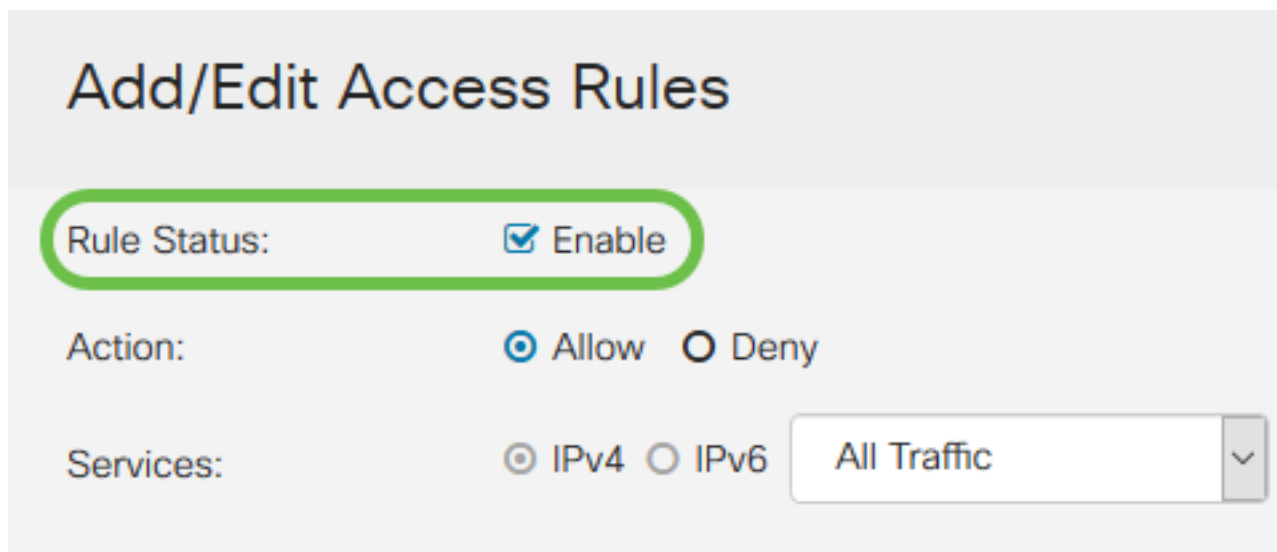
IPv4 Access Rules Table



<input checked="" type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	Any	Any	Any
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN

[Add/Edit Access Rules]ページが表示されます。

ステップ3:[Rule Status]のチェックボックスをオンまたはオフにして、動作中にアクセスルールを有効または無効にします。これは、後で適用するために保存するアクセスルールがある場合に便利です。



Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

ステップ4:[Action]フィールドで、着信ネットワークトラフィックへのアクセスをルールで許可するか、拒否するかを指定します。

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

注：望ましくないトラフィックだけを拒否するのではなく、受信を想定するトラフィックだけを許可するアクセスルールを設定することが、最適なセキュリティを実現することをお勧めします。これにより、未知の脅威からネットワークを保護しやすくなります。

ステップ5:[サービス]フィールドで、アクセスルールを適用するネットワークサービスのタイプをドロップダウンメニューから選択します。

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

注：[IPv4またはIPv6]オプションボタンは、[アクセスルール]ページからアクセスルールを適用するために選択したテーブルに基づいて自動的に選択されます。

ステップ6:[Log] フィールドから、ネットワークに入るパケットが適用されたルールに一致した場合にルータでログメッセージを生成するかどうかを選択します。

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

ステップ7:[Source Interface]ドロップダウンリストから、アクセスルールが適用される着信パケットのネットワークインターフェイスを選択します。

Log: Always Never

Source Interface: Any

Source Address: WAN
USB
VLAN1
Any

Destination Interface: Any

Destination Address: Any

ステップ8:[Source Address]ドロップダウンリストから、アクセスルールを適用する着信アドレスのタイプを選択します。オプションは次のとおりです。

- [Any] : このルールは、すべての着信IPアドレスに適用されます
- Single : ルールは、単一の定義されたIPアドレスに適用されます
- サブネット : このルールは、ネットワークの定義されたサブネットに適用されます
- [IP範囲(IP Range)] : ルールは定義された範囲のIPアドレスに適用されます

注 : [Single]、[Subnet]、または[IP Range]を選択すると、対応するフィールドがドロップダウンメニューの右側に表示され、アドレスの詳細を入力できます。この例では、IP範囲を入力してデモンストレーションを行います。

Source Interface: Any

Source Address: IP Range 1.2.3.1 To 1.2.3.100 (1.2.3.1 To 1.2.3.4)

Destination Interface: Any
Single
Subnet
IP Range

Destination Address:

ステップ9:[Destination Interface] ドロップダウンリストから、アクセスルールが適用される発信

パケットのネットワークインターフェイスを選択します。

Log: Always Never

Source Interface: Any

Source Address: Any

Destination Interface: Any

Destination Address:

Schedule

ステップ10:[Destination Address]ドロップダウンリストから、アクセスルールが適用される発信アドレスのタイプを選択します。オプションは次のとおりです。

- [Any] : このルールは、すべての発信IPアドレスに適用されます
- Single : ルールは、単一の定義されたIPアドレスに適用されます
- サブネット : このルールは、ネットワークの定義されたサブネットに適用されます
- [IP範囲(IP Range)] : ルールは定義された範囲のIPアドレスに適用されます

注 : [Single]、[Subnet]、または[IP Range]を選択すると、対応するフィールドがドロップダウンメニューの右側に表示され、アドレスの詳細を入力できます。この例では、サブネットを入力して説明します。

Destination Interface: Any

Destination Address: Subnet 1.2.3.4 / 16 (1.2.3.4 / 32)

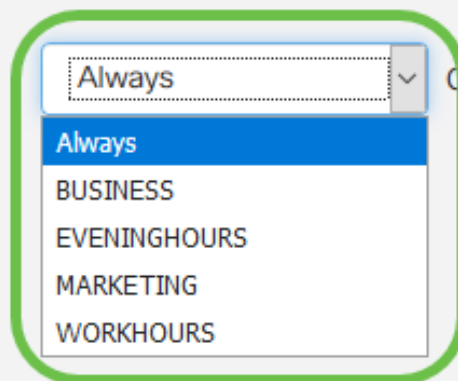
Schedule

Schedule Name: Always Click [here](#) to configure the schedules.

ステップ11:[スケジュール名]ドロップダウンリストから、アクセスルールを適用するタイムスケジュールを選択します。

Schedule

Schedule Name:

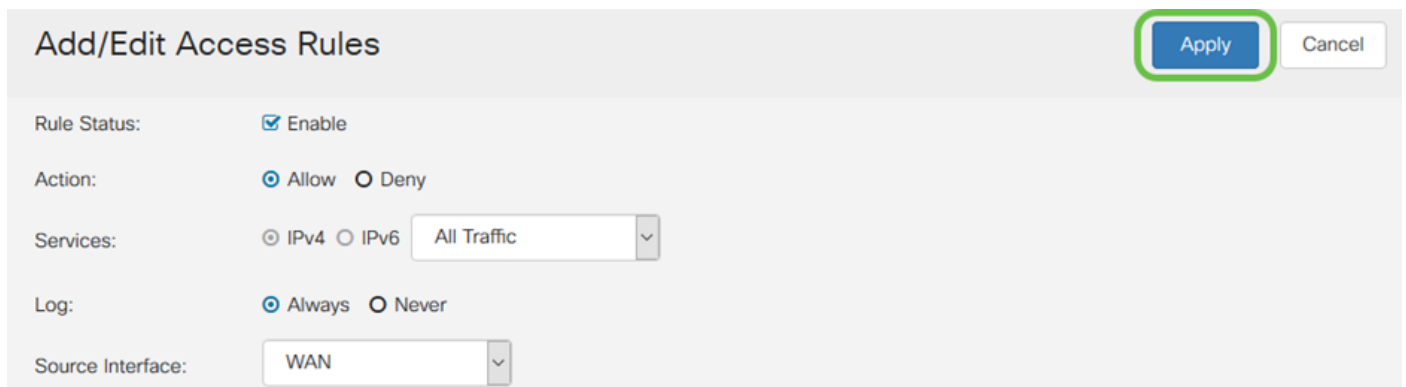


[Click here](#) to configure the schedules.

注：セキュリティを強化するには、ビジネスが稼働していないときに不要な接続が拒否されるように、重要でないネットワークアクセスを営業時間に制限することがベストプラクティスです。

注：アクセスルールのスケジュール時間を設定する場合は、[スケジュール名]ドロップダウンの右側にあるリンクをクリックします。これらのスケジュールの設定方法については、[こちらをご覧ください](#)。

ステップ12：アクセスルールの設定に問題がなければ、[Apply]をクリックして確認してください。




これで、メインの[アクセスルール]ページに戻ります。

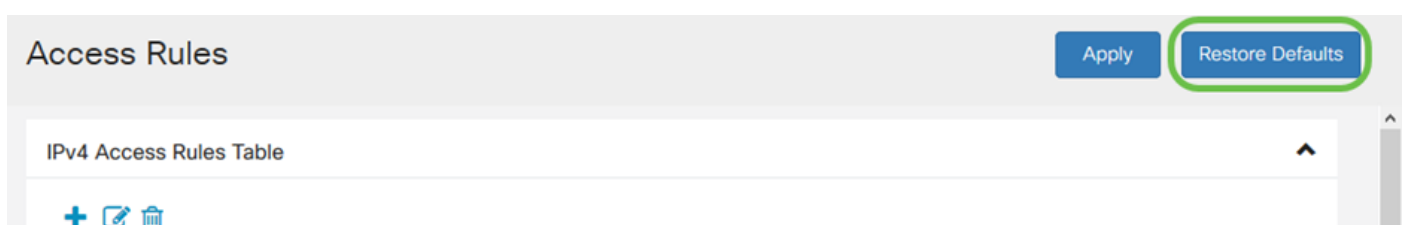
注：新しいアクセスルールが作成されると、その優先度がリストの一番下に配置されます。つまり、特定のパラメータでアクセスルールが他のアクセスルールと競合する場合、優先順位の高いルールの制限が優先されます。ルールを優先度の上または下に移動するには、[Configure]列にある青い矢印を使用します。

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	

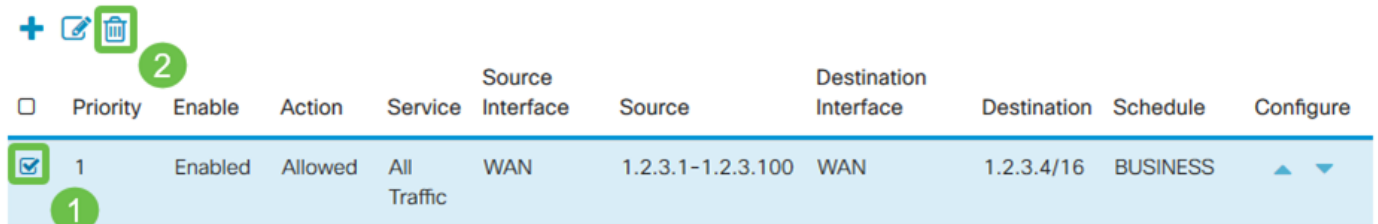
ステップ 13 (オプション)：アクセス規則の一覧を既定に戻す場合は、ページの右上隅にある[既定に戻す]をクリックします。



アクセスルールの削除

ステップ14：リストからアクセスルールを削除するには、削除する対応するルールのチェックボックスをオンにします。リストの上部にある青いゴミ箱アイコンを選択します。複数のアクセスルールエントリを一度に削除できます。

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	▲ ▼

Service Management

サービス管理を使用すると、ポート番号、プロトコル、およびその他の詳細に基づいて、既存のネットワークサービスを追加または編集できます。これらのネットワークサービスは、アクセスルールを設定するときに[サービス(Services)]ドロップダウンで使用できます。サービス管理リストの設定メニューを使用して、カスタムサービスを作成し、アクセスルールに適用して、ネットワークに入るトラフィックをより細かく制御できます。サービス管理の構成方法の詳細については、[ここをクリックしてください](#)。

結論

適切に適用されたアクセスルールは、WAN接続を保護するための貴重なツールです。上記のガイドと説明されているプラクティスを使用して、RV160xまたはRV260xルータのセキュアアクセスルールを適切に設定するために必要な情報をすべて入手する必要があります。