

RV34xシリーズルータのアクセスルールの設定

目的

RV340 Dual-WAN VPNルータは、使いやすく、柔軟性に優れた高性能デバイスで、スモールビジネスに最適です。Webフィルタリング、アプリケーション制御、IPソースガードなどのセキュリティ機能を追加。新しいRV340は、小規模オフィスやリモートの従業員に対して、安全性の高いブロードバンド接続を提供します。これらの新しいセキュリティ機能により、ネットワーク上で許可されたアクティビティを微調整することも容易になります。

RV34xシリーズルータのアクセスルールまたはポリシーを使用すると、ルールを設定してネットワークのセキュリティを強化できます。ルールの組み合わせであり、アクセスコントロールリスト(ACL)を使用している。ACLは、特定のユーザとの間で送受信されるトラフィックをブロックまたは許可するリストです。アクセスルールは、常に有効になるように、または定義されたスケジュールに基づいて設定できます。

ACLはリストの最後に暗黙のdenyがあるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザがルータ経由でネットワークにアクセスできるようにするには、特定のアドレスを拒否し、その他すべてのアドレスを許可する必要があります。

この記事の目的は、RV34xシリーズルータでアクセスルールを設定する方法を示すことです。

該当するデバイス

- RV34xシリーズ

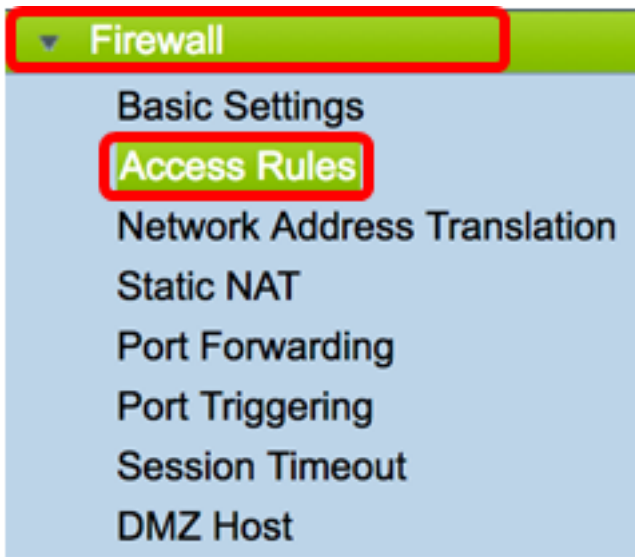
[Software Version]

- 1.0.1.16
 - [この記事の公開以降、UIを更新するファームウェアが利用可能になりました。ここをクリックしてダウンロードページにアクセスし、該当する製品を探してください。](#)

RV34xシリーズルータのアクセスルールの設定

アクセスルールの作成

ステップ1：ルータのWebベースのユーティリティにログインし、[Firewall] > [Access Rules]を選択します。

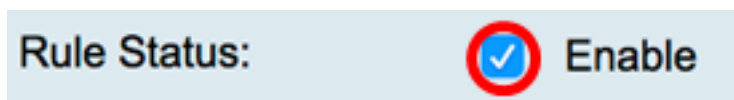


ステップ2:[IPv4またはIPv6アクセスルール(IPv4 or IPv6 Access Rules)]テーブルで、[追加(Add)]をクリックして新しいルールを作成します。

注：RV34xシリーズルータでは、最大202のルールを設定できます。この例では、IPv4が使用されています。

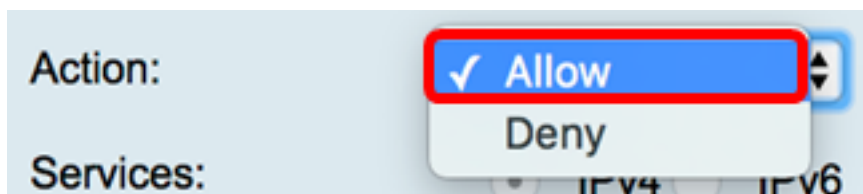


ステップ3:[Enable Rule Status]チェックボックスをオンにして、ルールを有効にします。



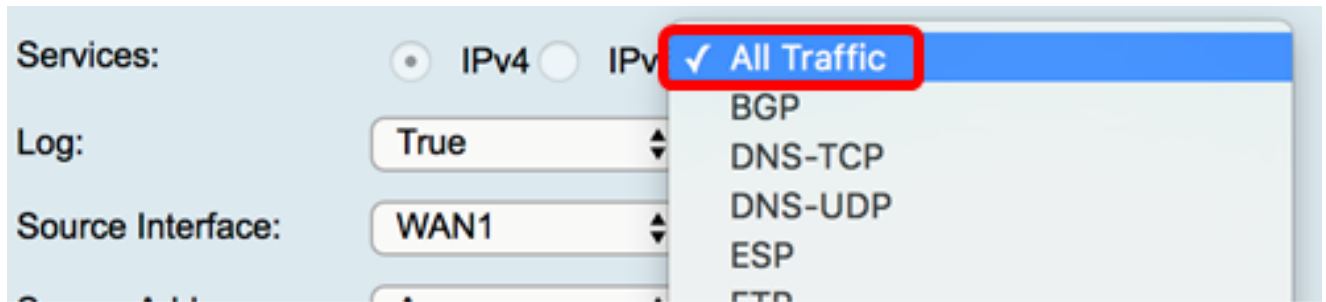
ステップ4:[Action (アクション)]ドロップダウンメニューで、ポリシーがデータを許可するか拒否するかを選択します。

注：この例では、[Allow]が選択されています。



ステップ5:[Services]ドロップダウンメニューから、ルータが許可または拒否するトラフィックの種類を選択します。

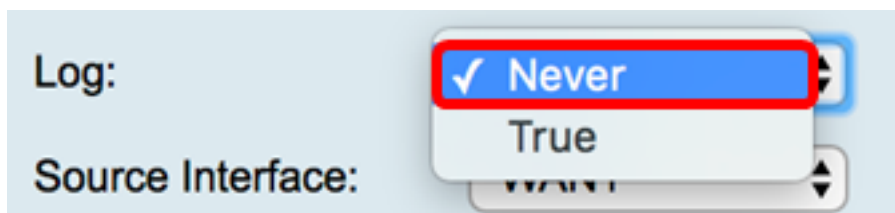
注：この例では、[All traffic]が選択されています。すべてのトラフィックが許可されます。



ステップ6:[Log]ドロップダウンメニューから、許可または拒否されたトラフィックをルータがログに記録するかどうかを判断するオプションを選択します。次のオプションがあります。

- Never：ルータは、許可および拒否されたトラフィックをログに記録しません。
- True：ルータはポリシーに一致するトラフィックをログに記録します。

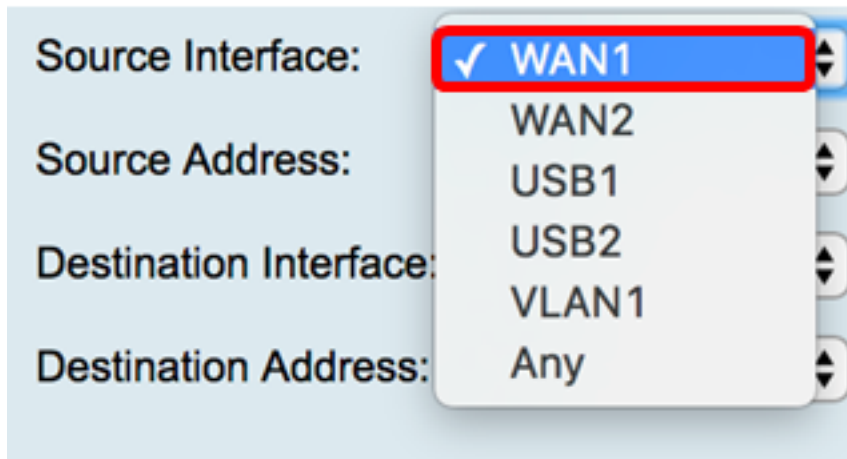
注：この例では、[Never]が選択されています。



ステップ7:[Source Interface]ドロップダウンメニューから、アクセスポリシーを適用する着信トラフィックまたは着信トラフィックのインターフェイスを選択します。オプションは次のとおりです

- WAN1：ポリシーはWAN1からのトラフィックにのみ適用されます。
- WAN2：ポリシーはWAN2からのトラフィックにのみ適用されます。
- USB1：ポリシーはUSB1からのトラフィックにのみ適用されます。
- USB2：ポリシーはUSB2からのトラフィックにのみ適用されます。
- VLAN1：ポリシーはトラフィックVLAN1だけに適用されます。
- Any：ポリシーは任意のインターフェイスに適用されます。

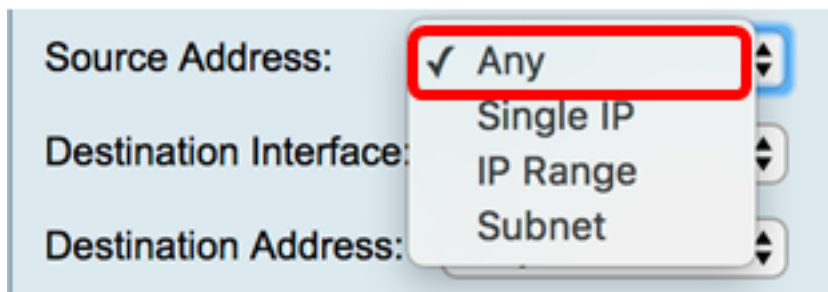
注：追加の仮想ローカルエリアネットワーク(VLAN)が設定されている場合、リストにVLANオプションが表示されます。この例では、WAN1が選択されています。



ステップ8:[Source Address]ドロップダウンメニューから、ポリシーを適用するソースを選択します。次のオプションがあります。

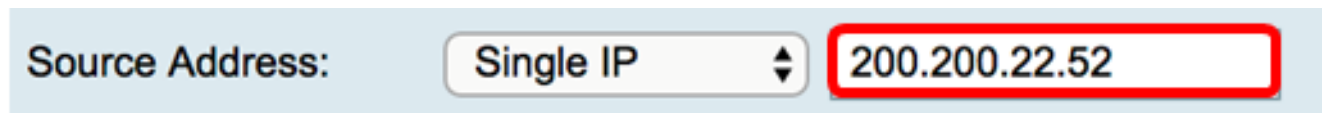
- [任意(Any)]：ポリシーはネットワーク上の任意のIPアドレスに適用されます。これを選択した場合は、ステップ12に進みます。
- Single IP：ポリシーは、1つのホストまたはIPアドレスに適用されます。これを選択した場合は、ステップ9に進みます。
- [IP範囲(IP Range)]：ポリシーは、IPアドレスのセットまたは範囲に適用されます。これを選択した場合は、ステップ10に進みます。
- サブネット：ポリシーはサブネットワーク全体に適用されます。これを選択した場合は、ステップ11に進みます。

注：この例では、[Any]が選択されています。



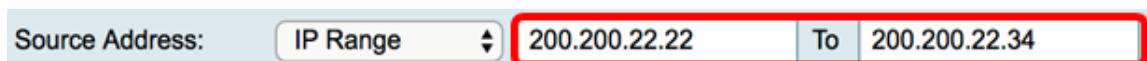
[ステップ9:\(オプション\)](#)ステップ8で単一のIPを選択し、適用するポリシーの単一のIPアドレスを入力し、ステップ12に進みます。

注：この例では、200.200.22.52が使用されています。



[ステップ10:\(オプション\)](#)ステップ8でIP範囲を選択した場合は、それぞれのIPアドレスフィールドに開始IPアドレスと終了IPアドレスを入力します。

注：この例では、200.200.22.22が開始IPアドレスとして使用され、200.200.22.34が終了IPアドレスとして使用されています。



[ステップ11:\(オプション\)](#)ステップ8で[Subnet]を選択した場合は、ネットワークIDとそれぞ

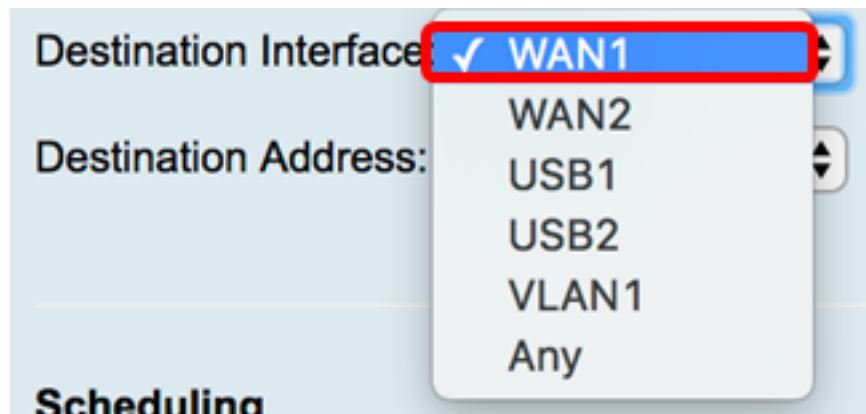
れのサブネットマスクを入力して、ポリシーを適用します。

注：この例では、サブネットIDとして200.200.22.1が、サブネットマスクとして24が使用されています。



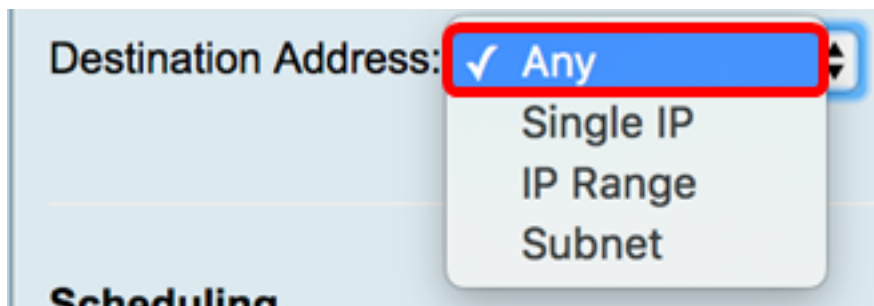
ステップ12: [Destination Interface]ドロップダウンメニューから、アクセスポリシーを適用する発信トラフィックまたは発信トラフィックのインターフェイスを選択します。オプションは、WAN1、WAN2、USB1、USB2、VLAN1、およびAnyです。

注：この例では、WAN1が選択されています。



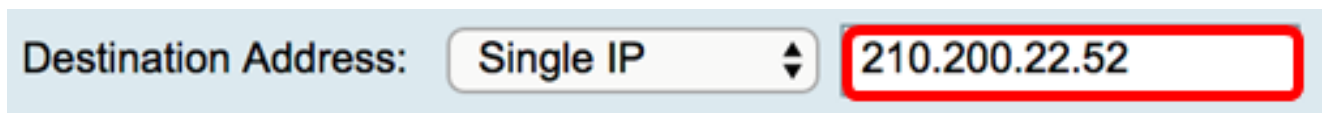
ステップ13:[Destination Address]ドロップダウンメニューから、ポリシーを適用する宛先を選択します。オプションは、[Any]、[Single IP]、[IP Range]、[Subnet]です。

注：この例では、[Any]が選択されています。ステップ 17 に進みます。



ステップ14: (オプション) ステップ13で[Single IP]を選択した場合は、適用するポリシーのIPアドレスを1つ入力します。

注：この例では、210.200.22.52が使用されています。



ステップ15: (オプション) ステップ13でIP範囲を選択した場合は、それぞれのIPアドレスフィールドに開始IPアドレスと終了IPアドレスを入力します。

注：この例では、210.200.27.22が開始IPアドレスとして使用され、210.200.27.34が終了IPアドレスとして使用されています。ステップ 17 に進みます。

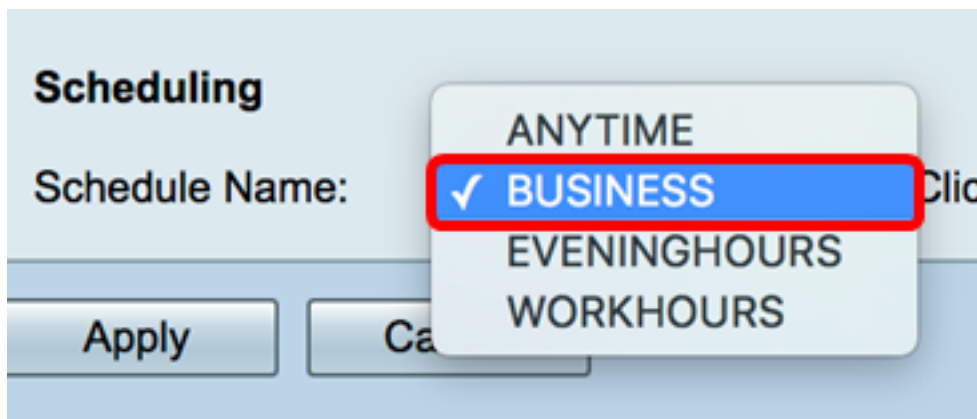
Destination Address: IP Range 210.200.27.22 To 210.200.27.34

ステップ16: (オプション) ステップ13で[Subnet]を選択した場合は、ネットワークアドレスとそれぞれのサブネットマスクを入力して、ポリシーを適用します。

注：この例では、210.200.27.1がサブネットアドレスとして、24がサブネットマスクとして使用されています。

Destination Address: Subnet 210.200.27.1 / 24

[ステップ17](#):[\[スケジュール名\]](#)ドロップダウンリストから、このポリシーを適用するスケジュールを選択します。スケジュールの設定方法については、[ここをクリックしてください](#)。



ステップ18:[Apply]をクリックします。

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

これで、RVシリーズルータにアクセスルールが正常に作成されました。

アクセスルールの編集

ステップ1:IPv4またはIPv6アクセスルールテーブルで、設定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。

注：この例では、[IPv4 Access Rules Table]で[Priority 1]が選択されています。

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

ステップ2:[Edit]をクリックします。

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

ステップ3: (オプション) [Configure]列で、目的のアクセスルールの行にある[Edit]ボタンをクリックします。

Schedule	Configure			
BUSINESS	<input checked="" type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
BUSINESS	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

ステップ4: 必要なパラメータを更新します。

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

Apply

Cancel

ステップ5:[Apply]をクリックします。

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

ステップ6: (オプション) [設定]列のアクセスルールの優先順位を変更するには、移動するアクセスルールの[上へ]ボタンまたは[下へ]ボタンをクリックします。

注：アクセスルールを上または下に移動すると、元の配置の1ステップ上または下に移動します。この例では、プライオリティ1が下に移動します。

Priority	Enable	Action	Service	Source Interf...	Source	Destinat...	Destination	Schedule	Configure
1	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	WAN1	Any	USB1	192.168.1.1	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
201	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	VLAN	Any	WAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
202	<input checked="" type="checkbox"/>	Denied	IPv4: All T...	WAN	Any	VLAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>

注：この例では、Priority 1がPriority 2になっています。

IPv4 Access Rules Table										
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter...	Source	Destina...	Destination	Schedule	Configure
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	VLAN	Any	WAN	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Tr...	WAN	Any	VLAN	Any	ANYTIME	Edit Delete Up Down

Add Edit Delete

ステップ7:[Apply]をクリックします。

Access Rules

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inte
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Add Edit Delete

IPv6 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inte
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

Add Edit Delete

これで、RV34xシリーズルータのアクセスルールが正常に編集されました。

アクセスルールの削除

ステップ1:IPv4またはIPv6アクセスルールテーブルで、削除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。

注：この例では、[IPv4 Access Rules Table]で[Priority 1]が選択されています。

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

ステップ2：テーブルの下にある[削除]をクリックするか、[設定]列の[削除]ボタンをクリックします。

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

ステップ3:[Apply]をクリックします。

Access Rules

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

IPv6 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

これで、RV34xシリーズルータのアクセスルールが正常に削除されたはずです。

[この記事に関連するビデオを表示...](#)

シスコのその他のテクニカルトピックを表示するには、[ここをクリックしてください](#)