RV34xシリーズルータの基本的なファイアウォール設定

目的

この記事の目的は、RV34xシリーズルータの基本的なファイアウォール設定の設定方法を説明することです。

概要

ファイアウォールの主な目的は、データパケットを分析し、事前に決められたルールセットに基づいて通過を許可するかどうかを決定することによって、着信および発信ネットワークトラフィックを制御することです。ルータは、着信データのフィルタリングを可能にする機能により、強力なハードウェアファイアウォールと見なされます。ネットワークファイアウォールは、セキュアで信頼できると想定される内部ネットワークと、セキュアで信頼できないと想定されるインターネットなどの外部インターネットワークとの間にブリッジを構築します。

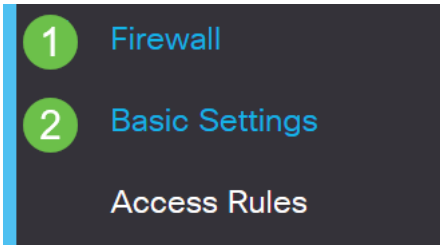
該当するデバイス |ファームウェアのバージョン

- RV34xシリーズ | 1.0.03.21 **（最新バージョンのダウンロード）**

ファイアウォールの基本設定

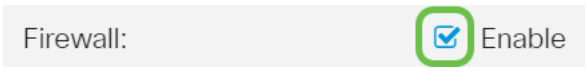
手順 1

Web User Interface (UI)にログインし、[Firewall] > [**Basic Settings**]**を選択します。**



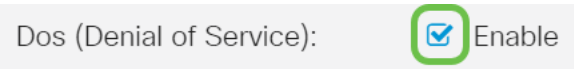
手順 2

[ファイアウォールを有効**にする**]チェックボックスをオンにして、ファイアウォール機能をアクティブにします。このコマンドはデフォルトで有効になっています。



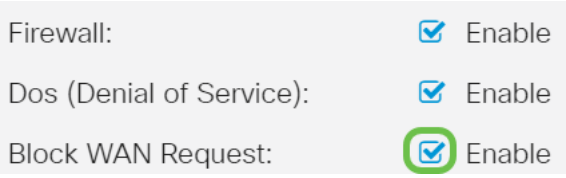
手順 3

DoS攻撃に対してネットワークを保護するには、[Dos（サービス拒否）を有効にする]チェックボックスをオンにします。このコマンドはデフォルトで有効になっています。



手順 4

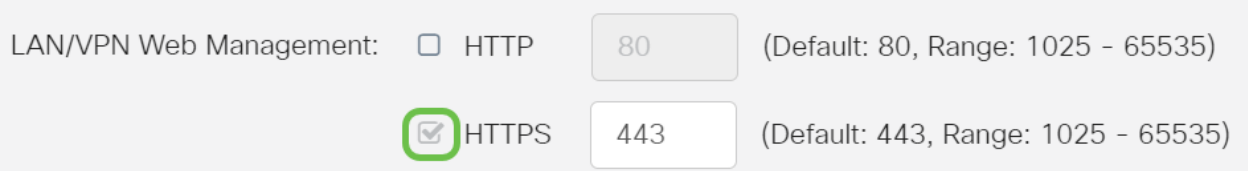
RV34xシリーズルータへのping要求を拒否するには、[Enable Block WAN Request]チェックボックスをオンにします。このコマンドはデフォルトで有効になっています。



手順 5

[LAN/VPN Web Management]領域で、[HTTP]チェックボックスまたは[HTTPS]チェックボックスをオンにして、これらのプロトコルからのトラフィックを有効にします。この例では、[HTTPS]チェックボックスがオンになっています。

- HTTP:Hyper Text Transfer Protocol（HTTP；ハイパーテキスト転送プロトコル）は、インターネットで使用されるデータ転送プロトコルです。
- HTTPS:Hyper Text Transfer Protocol Secureは、セキュリティを強化するためにパケットを暗号化するHTTPの安全なバージョンです。

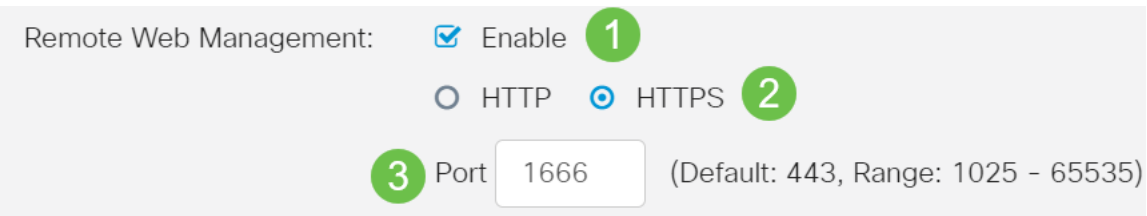


ステップ 6（オプション）

リモート管理を有効にするには、[リモートWeb管理を有効にする]チェックボックスをオンにします。それ以外の場合は、ステップ 8 に進みます。

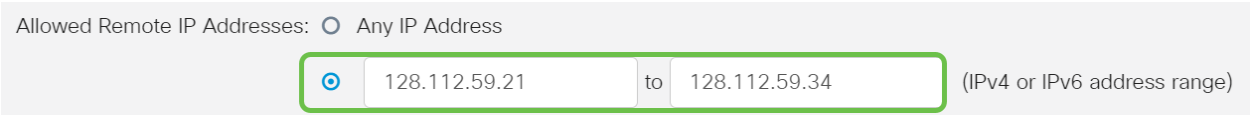
オプションボタンを選択して、ファイアウォールへの接続に使用するプロトコルのタイプを選択します。オプションはHTTPとHTTPSです。

リモート管理が許可される1025 ~ 65535の範囲のポート番号を入力します。デフォルトは443です。この例では、1666が使用されます。



ステップ7

[許可されたリモートIPアドレス(Allowed Remote IP Addresses)]領域で、任意のIPアドレスによるネットワークへのリモートアクセスを許可するか、IPv4またはIPv6アドレスの範囲を指定するオプションボタンを選択します。この例では、[IP Range]が選択されています。この例では、開始IPアドレスは128.112.59.21、終了IPアドレスは128.112.59.34です。



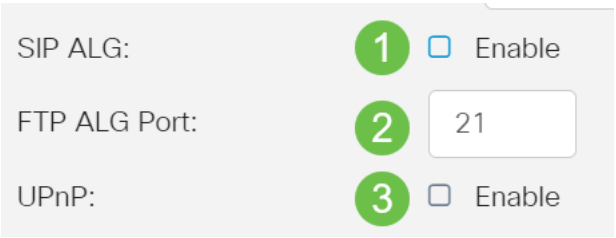
ステップ 8 (オプション)

[SIP ALGを有効にする]チェックボックスをオンにして、Session Initiation Protocol(SIP)アプリケーションレイヤゲートウェイ(ALG)がファイアウォールを通過できるようにします。この機能を有効にすると、SIPパケットがファイアウォールを通過しやすくなります。SIPパケットは、音声トラフィックの接続を開始するために使用されます。VoIPプロバイダーが別のネットワークアドレス変換(NAT)トラバーサルプロトコルを使用している場合、この機能を無効にできます。これはデフォルト設定です。

[FTP ALG Port]フィールドにSIP ALGのファイル転送プロトコル(FTP)ポートを指定します。デフォルト値は 21 です。

[UPnPを有効にする]チェックボックスをオンにして、ユニバーサルプラグアンドプレイ(UPnP)を有効にします。 この機能はデフォルトで無効になっています。

この例では、これらのオプションは無効のままになっています。



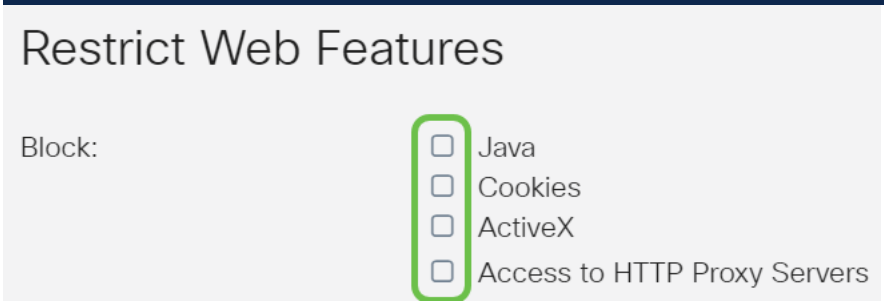
手順 9 (オプション)

[Restrict Web Feature]領域で、[Block]領域でブロックするWebフィーチャのタイプのチェックボックスをオンにします。これらのチェックボックスは、デフォルトでは無効になっています。次のオプションがあります。

Java：このタイプのWeb要素を含むすべてのWeb要素がブロックされます。この設定は、JavaベースのWeb攻撃の防止に役立ちます。
Cookie — Cookieは、Webサイトがアクセスしているユーザーを理解できるようにコンピュータに保存されるデータです。ブロックすると、悪意のあるCookieがデータにアクセスするのを防ぐことができます。
ActiveX：ブラウジングエクスペリエンスを向上させるためにMicrosoftによって開発されたプラグインです。これをブロックすると、悪意のあるActiveXプラグインがネットワークデバイスに害を及ぼすことを防止できます。
プロキシHTTPサーバへのアクセス：HTTPプロキシサーバは、エンドユーザの詳細をハッカーから隠します。クライアントがインターネットに直接アクセスしないように、仲介役として機能します。ただし、ローカルユーザがWANプロキシサーバにアクセス

できる場合、ルータ上のコンテンツフィルタを回避して、ルータによってブロックされたインターネットサイトにアクセスできる可能性があります。

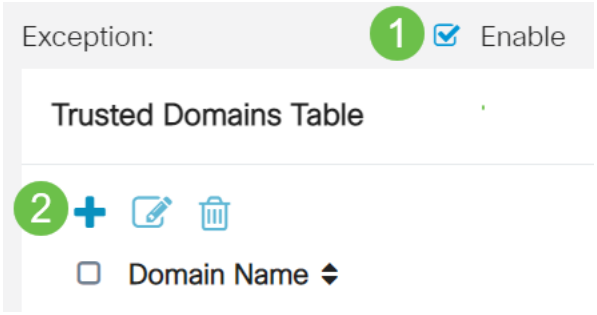
この例では、チェックボックスは無効のままにしておきます。



手順 11 (オプション)

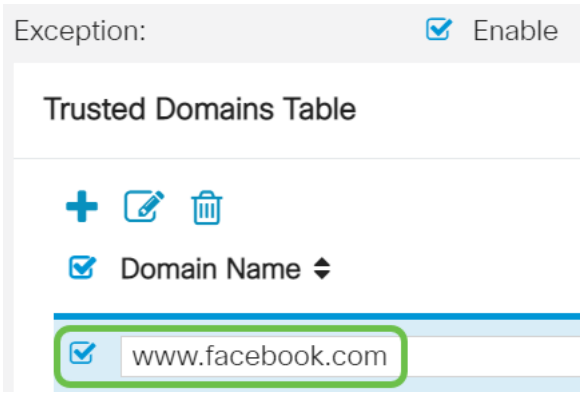
Java、Cookie、ActiveX、またはHTTPプロキシサーバへのアクセスなど、選択したWeb機能のみを許可し、その他すべてを制限するには、[例外を有効にする]チェックボックスをオンにします。これは、デフォルトでは無効になっています。この例では、無効のままにしておきます。

[信頼できるドメイン]テーブルで、[追加]アイコンをクリックし、ネットワーク上で信頼できるドメインまたはアクセスが許可されているドメインを追加します。



ステップ 12

[ドメイン*名*]フィールドに、ネットワークへのアクセスを許可するドメイン名を入力します。この例では、www.facebook.comを使用します。



手順 13

[Apply] をクリックします。

手順 14 (オプション)

構成を永続的に保存するには、[構成のコピー/保存]ページに移動するか、ページの上部にある保**存アイコン**をクリックします。

結論

これで、RV34xシリーズルータの基本的なファイアウォール設定が正常に設定されました。