RV215Wの基本的なファイアウォール設定

目的

ファイアウォールは、ネットワークのセキュリティを維持するために設計された一連の機能です。ルータは強力なハードウェアファイアウォールと見なされます。これは、ルータがすべての着信トラフィックを検査し、不要なパケットをドロップできるためです。

この記事では、RV215Wの基本的なファイアウォール設定の設定方法について説明します。

該当するデバイス

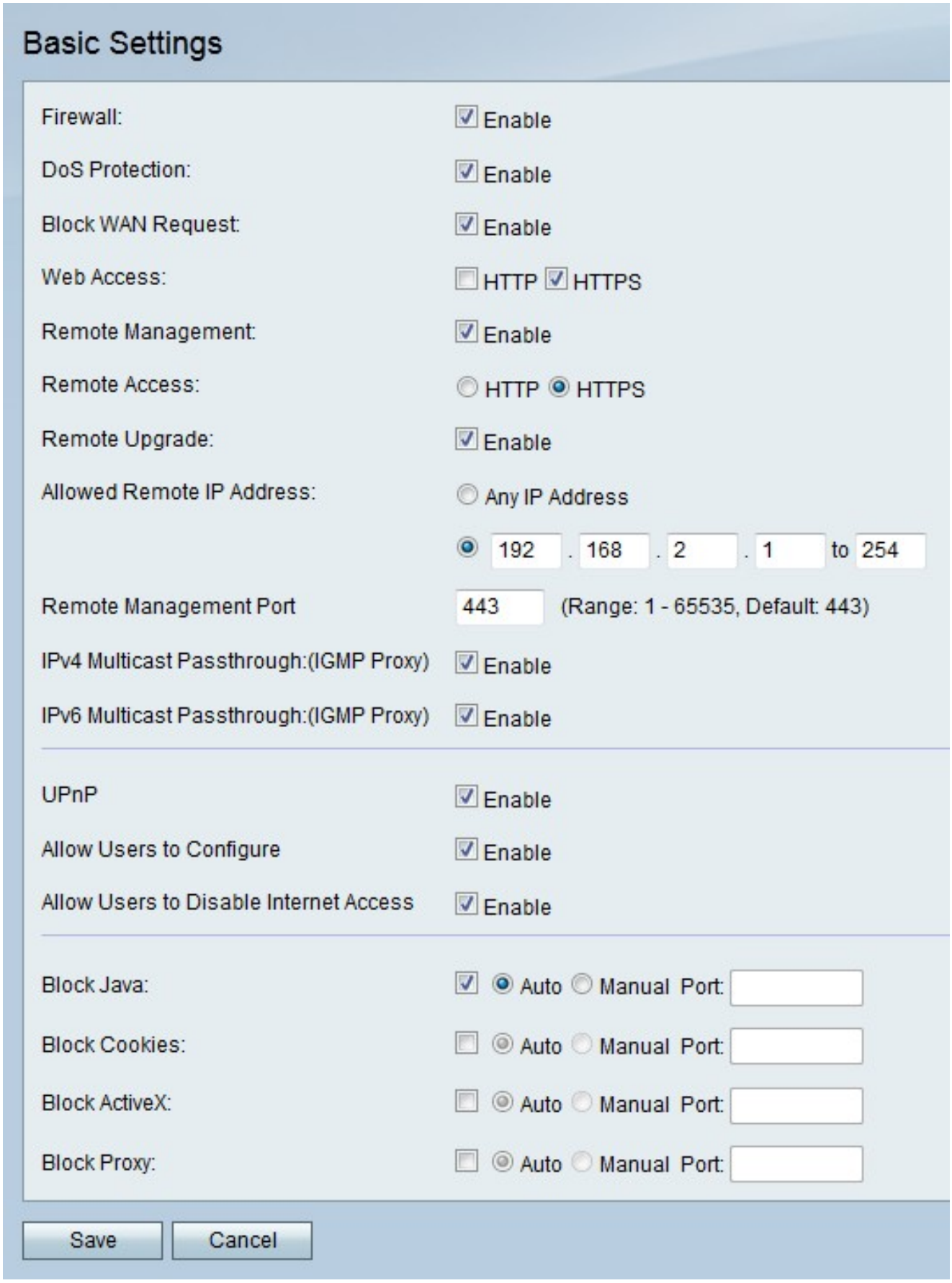
・ RV215W

[Software Version]

•1.1.0.5

基本設定

ステップ1:Web構成ユーティリティにログインし、[Firewall] > [Basic Settings]を選択します。[基本設定]ページが開きます。



ステップ2:[Firewall]フィールドの[Enable] をオンにして、RV215Wのファイアウォール設定を有効にします。

ステップ3:RV215Wでサービス拒否(DoS)保護を有効にするには、[DoS保護(DoS Protection)]フィールドの[有効(Enable)] をオンにします。DoS保護は、ネットワークがDistributed Denial of Service(DDoS)攻撃を受けないようにするために使用されます。

DDoS攻撃は、ネットワークのリソースが使用できなくなるような場所にネットワークをフラッディングすることを目的としています。RV215WはDoS保護を使用して、不要なパケットの制限と削除を通じてネットワークを保護します。

ステップ4:[Block WAN Request]フィールドの[Enable] をオンにして、WANからRV215Wへのすべてのping要求をブロックします。

ステップ5:[Web Access]フィールドで、ファイアウォールへの接続に使用できるWebアクセスの目的のタイプに対応するチェックボックスをオンにします。

ステップ6:[Remote Management]フィールドで[Enable]をオンにします。リモート管理により、リモートWANネットワークからRV215Wにアクセスできます。

ステップ7:[Remote Access]フィールドで、リモートWANからファイアウォールへの接続に使用できるWebアクセスの適切なタイプに対応するオプションボタンをクリックします。

ステップ8：リモートユーザがRV215Wをアップグレードできるように、[Remote Upgrade]をオンにします。

ステップ9:[Allowed Remote IP Address (許可されたリモートIPアドレス)]フィールドで、RV215Wへのリモートアクセスを許可するIPアドレスに対応するオプションボタンをクリックします。

- Any IP Address：すべてのIPアドレスが許可されます。
- IP Address：許可されるIPアドレスの範囲を入力します。

ステップ10:[Remote Management Port]フィールドに、リモートアクセスを許可するポートを入力します。リモートユーザは、リモートポートを使用してデバイスにアクセスする必要があります。

注：リモートアクセスの形式は、https://<*remote-ip*>:<*remote-port*>です

ステップ11:[IPv4 Multicast Passthrough]フィールドの[Enable] をオンにして、IPv4マルチキャストトラフィックがインターネットからRV215Wを通過できるようにします。IPマルチキャストは、単一の送信で指定された受信グループにIPデータグラムを送信するために使用される方法です。

ステップ12:[IPv6 Multicast Passthrough]フィールドの[Enable] をオンにして、IPv6マルチキャストトラフィックがインターネットからRV215Wを通過できるようにします。

ステップ13:[UPnP]フィールドの[Enable]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。UPnPを使用すると、RV215Wと通信できるデバイスを自動的に検出できます。

ステップ14:UPnP対応デバイスを持つユーザがUPnPポートマッピングルールを設定できるようにするには、[Allow Users to Configure]フィールドで[Enable] をオンにします。ポートマッピングまたはポートフォワーディングは、プライベートLAN内で提供される外部ホストとサービス間の通信を許可するために使用されます。

ステップ15:[Allow Users to Disable Internet Access]フィールドの[Enable] をオンにして、ユーザがデバイスへのインターネットアクセスを無効にします。

ステップ16:Block Javaをチェックし、Javaアプレットのダウンロードをブロックします。悪意のある目的のために作成されたJavaアプレットは、ネットワークにセキュリティ上の脅威を与える可能性があります。ダウンロードすると、悪意のあるJavaアプレットがネッ

トワークリソースを不正利用する可能性があります。目的のブロック方式に対応するオプションボタンをクリックします。

- Auto — Javaを自動的にブロックします。
- 手動ポート：Javaをブロックする特定のポートを入力します。

ステップ17:[Block Cookie]をオンにして、WebサイトによるCookieの作成を拒否します。Cookieは、これらのユーザの情報を保存するためにWebサイトによって作成されます。クッキーは、プライバシーの侵害につながる可能性のあるユーザのWeb履歴を追跡できます。目的のブロック方式に対応するオプションボタンをクリックします。

- Auto — Cookieを自動的にブロックします。
- 手動ポート：Cookieをブロックする特定のポートを入力します。

ステップ18:[Block ActiveX]をオンにして、ActiveXアプレットのダウンロードをブロックします。ActiveXは、セキュリティが欠けているアプレットの一種です。ActiveXアプレットがコンピュータにインストールされると、ユーザが行うことができることはすべて実行できます。オペレーティングシステムに有害なコードを挿入したり、安全なイントラネットをサーフィンしたり、パスワードを変更したり、ドキュメントを取得して送信したりすることがあります。目的のブロック方式に対応するオプションボタンをクリックします。

- Auto — ActiveXを自動的にブロックします。
- 手動ポート：ActiveXをブロックする特定のポートを入力します。

ステップ19：プロキシサーバをブロックするには、[プロキシのブロック]をオンにします。プロキシサーバは、2つの異なるネットワーク間のリンクを提供するサーバです。悪意のあるプロキシサーバは、ログインやパスワードなどの暗号化されていないデータを記録できます。目的のブロック方式に対応するオプションボタンをクリックします。

- Auto – プロキシサーバを自動的にブロックします。
- 手動ポート：プロキシサーバをブロックする特定のポートを入力します。

ステップ20:[Save]をクリックします。