RV130およびRV130Wの基本的なファイアウォール設定の設定方法

目的

ファイアウォールの基本設定を使用すると、デバイスが着信および発信インターネットトラフィックを選択的にブロックおよび許可するために使用するルールを作成および適用することによって、ネットワークを保護できます。
ユニバーサルプラグアンドプレイなどの機能により、追加の設定を行わなくても、ネットワーク上のデバイスを簡単に相互に接続できます。

ユニバーサルプラグアンドプレイ(UPnP)により、デバイスと通信できるデバイスを自動検出できます。コンテンツをブロックすると、特定のコンテンツがデバイスに送信され、セキュリティが侵害されたり、コンピュータが悪意のあるソフトウェアに感染したりする可能性があるため、コンピュータのセキュリティ保護に役立ちます。選択したポート上の特定のコンテンツをブロックする機能は、ファイアウォールセキュリティを強化するのに役立ちます。

このドキュメントの目的は、RV130およびRV130Wでファイアウォールの基本設定を行う方法を説明することです。

該当するデバイス

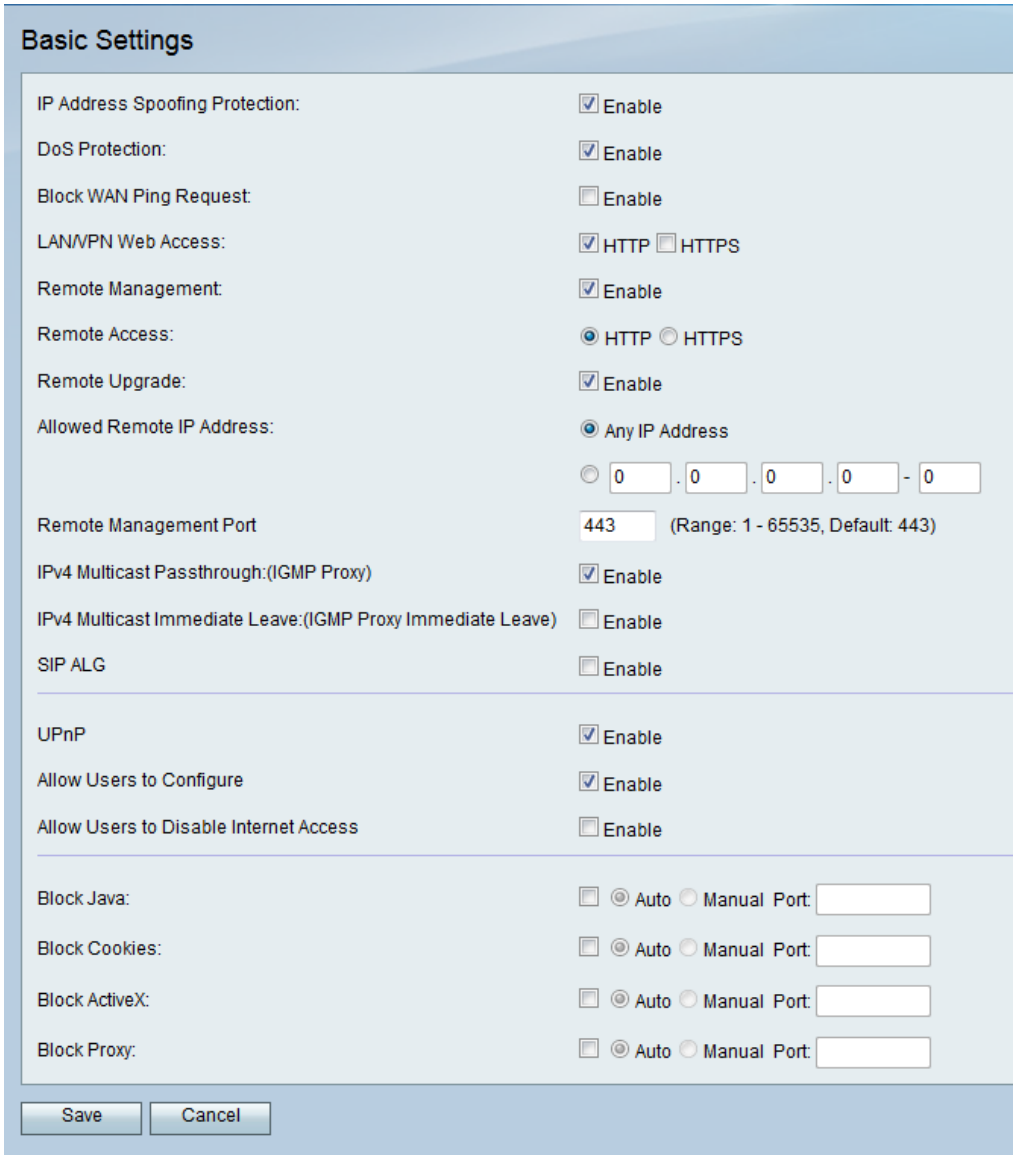
- RV130
- RV130W

[Software Version]

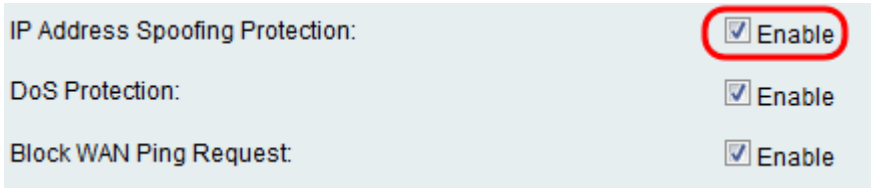
- v1.0.1.3

ファイアウォールの基本設定

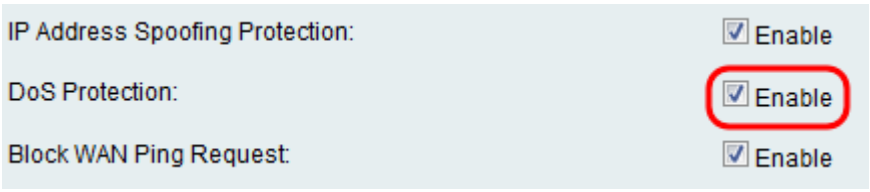
ステップ1:Web設定ユーティリティにログインし、[Firewall] > [Basic Settings] を選択します。[基本設定]ページが開きます。



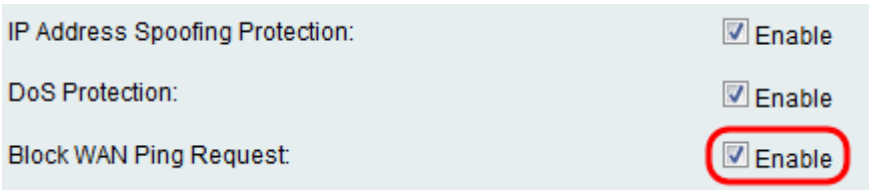
ステップ2:[IP Address Spoofing Protection] フィールドで、[Enable] チェックボックスをオンにして、IPアドレススプーフィングからネットワークを保護します。IPアドレスのスプーフィングとは、不正ユーザが自身のIPアドレスを使用して別の信頼できるデバイスになりすましてネットワークにアクセスしようとする場合です。有効にすることを推奨します。
IPアドレススプーフィング保護。



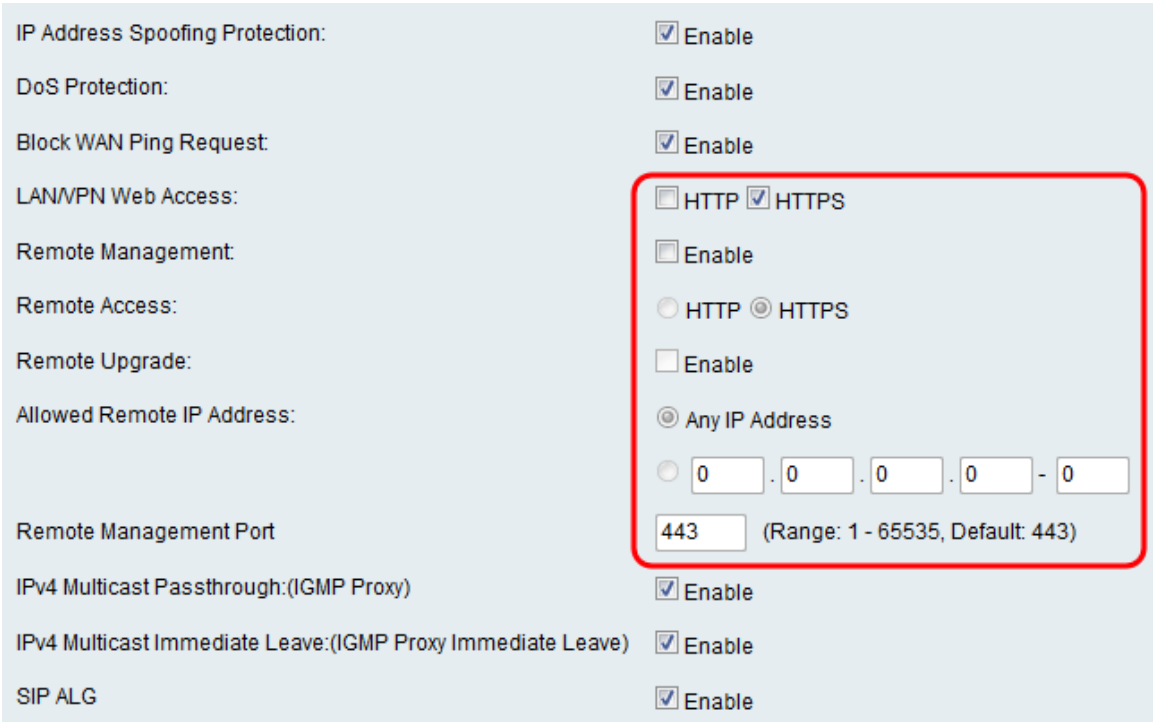
ステップ3:[DoS Protection] フィールドで、[Enable] チェックボックスをオンにして、ネットワークをサービス拒否攻撃から保護します。Denial of Service（DoS；サービス拒否）保護は、分散型サービス拒否(DDoS)攻撃からネットワークを保護するために使用されます。DDoS攻撃は、ネットワークのリソースが使用できなくなるまでネットワークをフラッディングすることを意味します。



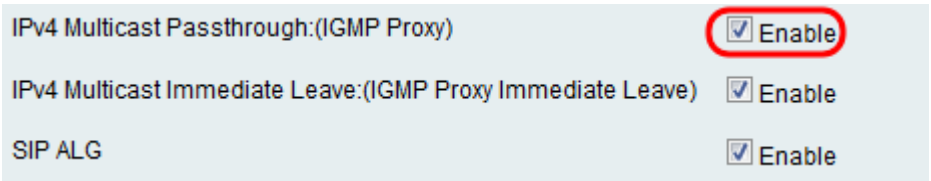
ステップ4:[Block WAN Ping Request] フィールドで、[Enable] チェックボックスをオンにして、外部WANネットワークからデバイスへのping要求を停止します。



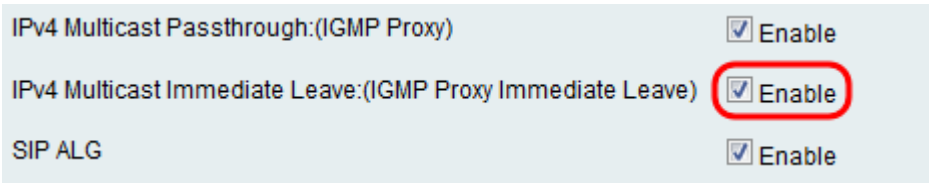
ステップ5:*LAN/VPN Webアクセスからリモート管理ポート*へのリストされたフィールドは、LANおよびリモート管理Webアクセスの設定に使用されます。これらの設定の詳細については、『RV130およびRV130WでのLANおよびリモート管理Webアクセスの設定』を参照してください。



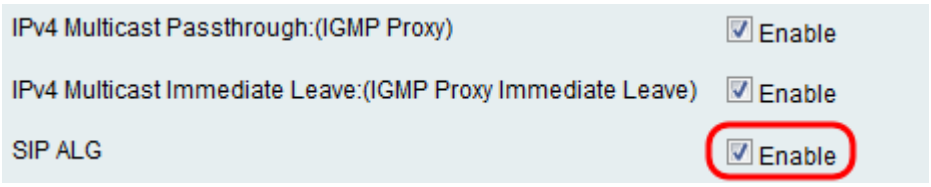
ステップ6:[IPv4 Multicast Passthrough:(IGMP Proxy)]フィールドで、[Enable] チェックボックスをオンにして、IPv4のマルチキャストパススルーを有効にします。これにより、外部WANネットワークから内部LANにグループIGMPパケットが転送されます。



ステップ7:[IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)] フィールドで、[Enable] チェックボックスをオンにして、マルチキャスト即時脱退を有効にします。即時脱退を有効にすると、マルチキャストグループが同時に使用されている間でも、ネットワーク上のホストに最適な帯域幅管理が提供されます。



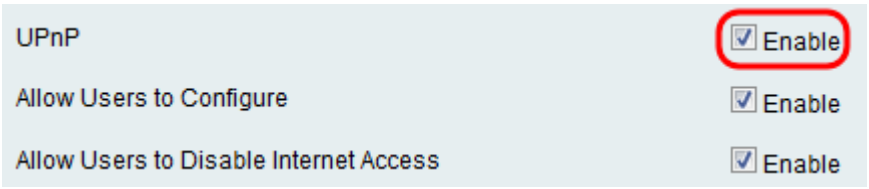
ステップ8:[Session Initiation Protocol (SIP) Application Layer Gateway (ALG)] フィールドで、[Enable] チェックボックスをオンにして、Session Initiation Protocol (SIP)トラフィックがファイアウォールを通過できるようにします。Session Initiation Protocol(SIP)は、IPネットワーク上で音声およびマルチメディアコールのセットアップを通知するプラットフォームを備えています。アプリケーションレイヤゲートウェイ(ALG)、またはアプリケーションレベルゲートウェイとも呼ばれるアプリケーションは、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。



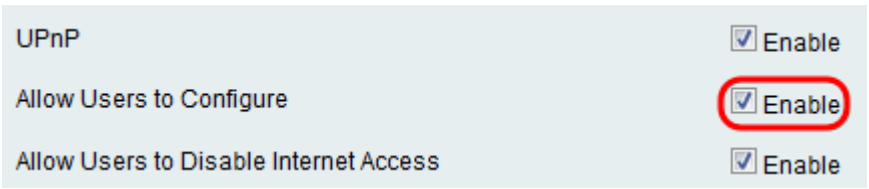
注：このデバイスは、最大256のSIP ALGセッションをサポートします。

ユニバーサルプラグアンドプレイの設定

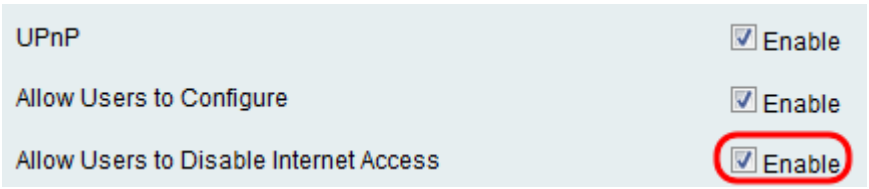
ステップ1:[UPnP] フィールドで、[Enable] をオンにしてユニバーサルプラグアンドプレイ(UPnP)を有効にします。



ステップ2:[Allow Users to Configure] フィールドで、[Enable] チェックボックスをオンにして、コンピュータまたは他のUPnP対応デバイスでUPnPサポートが有効になっているユーザがUPnPポートマッピングルールを設定できるようにします。無効にすると、デバイスはアプリケーションに転送ルールの追加を許可しません。



ステップ3:[Allow Users to Disable Internet Access] フィールドで、[Enable] チェックボックスをオンにして、ユーザがインターネットアクセスを無効にできるようにします。



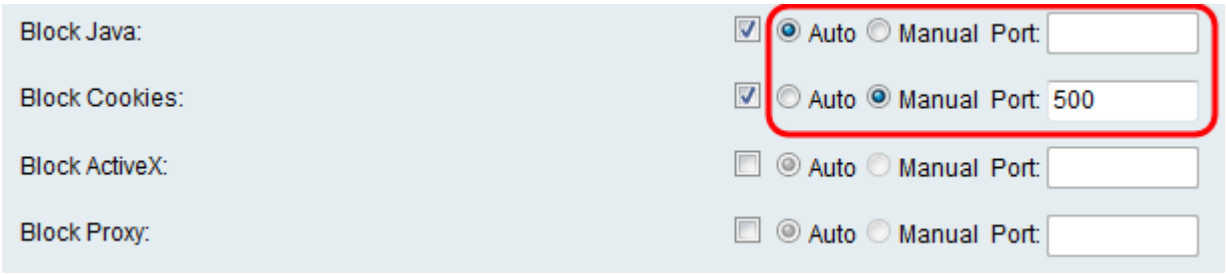
コンテンツのブロック

ステップ1：デバイスからブロックするコンテンツに対応するフィールドのチェックボックスをオンにします。

使用可能なオプションは次のように定義されています。

- Javaのブロック： Javaアプレットのダウンロードをブロックします。
- クッキーをブロックする：デバイスがWebページからクッキー情報を受信することをブロックします。
- ActiveXをブロック – WindowsオペレーティングシステムでInternet Explorerを使用しているときに存在する可能性があるActiveXアプレットをブロックします。
- プロキシのブロック：デバイスがプロキシサーバを介して外部デバイスと通信することをブロックします。これにより、デバイスがファイアウォールルールを回避できなくなります。

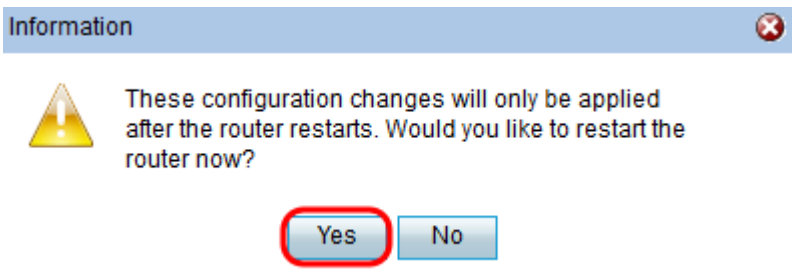
ステップ2:[Auto] オプションボタンを選択して、その特定のコンテンツのすべてのインスタンスを自動的にブロックするか、[Manual] オプションボタンをクリックし、コンテンツをブロックする対応するフィールドに特定のポートを入力します。



注：ポート値の範囲(1 ~ 65535)に任意の番号を入力できます。

ステップ3:[Save] をクリックして設定を保存します。

ステップ4：ウィンドウが表示され、ルータを再起動するように求められます。**Yes**をクリックしてルータを再起動し、変更を適用します。



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。