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。

Basic Settings	
IP Address Spoofing Protection:	Enable
DoS Protection:	✓ Enable
Block WAN Ping Request:	Enable
LAN/VPN Web Access:	ITTP HTTPS
Remote Management:	✓ Enable
Remote Access:	● HTTP ○ HTTPS
Remote Upgrade:	✓ Enable
Allowed Remote IP Address:	Any IP Address
	◎ 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	✓ Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	Enable
SIP ALG	Enable
UPnP	Tenable
Allow Users to Configure	✓ Enable
Allow Users to Disable Internet Access	Enable
Block Java:	🗐 🖲 Auto 🔿 Manual Port:
Block Cookies:	🗐 🖲 Auto 🔘 Manual Port:
Block ActiveX:	🗐 🔘 Auto 🔘 Manual Port:
Block Proxy:	Auto Manual Port:
Save Cancel	

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。*

IP Address Spoofing Protection:	🗵 Enable
DoS Protection:	Enable
Block WAN Ping Request:	Enable

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。

IP Address Spoofing Protection:	Enable
DoS Protection:	🗷 Enable
Block WAN Ping Request:	C Enable

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。

IP Address Spoofing Protection:	🗹 Enable
DoS Protection:	Enable
Block WAN Ping Request:	🛛 Enable

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、『<u>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</u>』を参照し てください。

IP Address Spoofing Protection:	Enable	
DoS Protection:	C Enable	
Block WAN Ping Request:	✓ Enable	
LAN/VPN Web Access:	HTTP I HTTPS	
Remote Management:	Enable	
Remote Access:	○ HTTP	
Remote Upgrade:	Enable	
Allowed Remote IP Address:	Any IP Address	
	0.0.0.0-0	
Remote Management Port	443 (Range: 1 - 65535, Default: 443)	
IPv4 Multicast Passthrough:(IGMP Proxy)	🗹 Enable	
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	✓ Enable	
SIP ALG	✓ Enable	

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。

IPv4 Multicast Passthrough:(IGMP Proxy)	🗹 Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	Enable
SIP ALG	Enable

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。

IPv4 Multicast Passthrough:(IGMP Proxy)	Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	🗷 Enable
SIP ALG	Enable

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。

IPv4 Multicast Passthrough:(IGMP Proxy)	🗹 Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	🗹 Enable
SIP ALG	🛛 Enable

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。

UPnP	🛛 Enable
Allow Users to Configure	Enable
Allow Users to Disable Internet Access	Enable

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。

UPnP	Cenable Enable
Allow Users to Configure	Enable
Allow Users to Disable Internet Access	Enable

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。

UPnP	🗹 Enable
Allow Users to Configure	🗹 Enable
Allow Users to Disable Internet Access	Enable



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。

Block Java:	Auto O Manual Port:
Block Cookies:	🖲 Auto 🔘 Manual Port:
Block ActiveX:	🖲 Auto 🔿 Manual Port:
Block Proxy:	Auto Manual Port:

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。

Block Java:	🗹 🖲 Auto 🔘 Manual Port:
Block Cookies:	🗹 🔿 Auto 🖲 Manual Port: 500
Block ActiveX:	Auto Manual Port:
Block Proxy:	🔲 🖲 Auto 🔿 Manual Port:

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。

Informatio	on	3
A	These configuration changes will only be applied after the router restarts. Would you like to restart the router now?	
	Yes No	

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。