

RV016、RV042、RV042G、およびRV082 VPNルータの一般的なファイアウォール設定

目的

ファイアウォールは、インターネットなどの外部ネットワークから内部ネットワークを保護します。ファイアウォールはネットワークセキュリティに不可欠です。セキュリティのニーズに基づいて特定のサービスを有効または無効にできる、いくつかの異なる設定を使用できます。

この記事の目的は、RV016、RV042、RV042G、およびRV082 VPNルータの一般的なファイアウォール設定を有効または無効にする方法を示すことです。

適用可能なデバイス

- ・ RV016
- ・ RV042
- ・ RV042G
- ・ RV082

[Software Version]

- ・ v4.2.1.02

一般的なファイアウォール設定

ステップ 1：ルータ設定ユーティリティにログインし、Firewall > Generalの順に選択します。Generalページが開きます。

General

Firewall :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
SPI (Stateful Packet Inspection) :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
DoS (Denial of Service) :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Block WAN Request :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Remote Management :	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Port : <input type="text" value="443"/>
HTTPS :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Multicast Passthrough :	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	

Restrict Web Features

Block :	<input type="checkbox"/> Java
	<input type="checkbox"/> Cookies
	<input type="checkbox"/> ActiveX
	<input type="checkbox"/> Access to HTTP Proxy Servers
	<input type="checkbox"/> Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.com

ステップ 2 : EnableまたはDisableオプションボタンをクリックして、ユーザの要件に応じてファイアウォールで使用可能な設定を有効または無効にします。

次のフィールドについて説明します。

- ・ **ファイアウォール** : この機能を有効にすると、ルータはこのルータを通過するすべてのトラフィックに対してディープパケットインスペクションを実行し、事前定義されたプロトコル動作に従わないパケットをドロップします。
- ・ **SPI (ステートフルパケットインスペクション)** : ルータのファイアウォールは、ステートフルパケットインスペクション(SPI)を使用して、ファイアウォールでトラフィックを確認します。TCPストリームやUDP通信などのネットワーク接続の状態を監視します。ファイアウォールは接続の種類ごとに正当なパケットを区別し、既知のアクティブな接続に一致するパケットだけがファイアウォールによって許可され、他のパケットはすべて拒否されます。

- ・ Dos (サービス拒否) : この機能を有効にすると、ルータはインターネットからのDOS (サービス拒否) 攻撃を防止します。DOS攻撃によってルータのCPUがビジー状態になり、通常のトラフィックにサービスを提供できなくなります。
- ・ WAN要求のブロック : これが有効な場合、ルータはインターネットからのPING要求を無視するため、隠れたように見えます。これは、ネットワークポートを隠すことでセキュリティを提供し、侵入者がネットワークに簡単にアクセスできないようにします。
- ・ リモート管理 : この機能を有効にすると、ルータはインターネットからWeb設定ユーティリティにアクセスすることを許可します。WAN側のホストに対して開くポート番号を入力します。デフォルト設定は 443 です。このポートは、ユーザがリモート接続を確立するときに指定する必要があります。
- ・ HTTPS : 有効にすると、通常のHTTPではなくWAN側からHTTPSセッションを介してWeb構成ユーティリティにアクセスできます。これにより、リモートWebセッションがSSL暗号化アルゴリズムによって保護されます。HTTPS機能が無効になっている場合、ユーザはQuickVPNを使用して接続できません。無効にした場合は、安全性の低いHTTP接続が使用されます。
- ・ マルチキャストパススルー : IGMPプロキシが現在ルータで実行されている場合、マルチキャストパススルーが有効にされると、ルータはインターネットからのIPマルチキャストトラフィックの受信を許可します。

注 : ファイアウォールを無効にするには、管理者パスワードをデフォルトから変更する必要があります。SPI (ステートフルパケットインスペクション)、DoS (サービス拒否)、Block WAN Request、およびRemote Managementの各フィールドはグレー表示されます。

ステップ 3 : 「Web機能の制限」領域で、対応する機能を制限する一部またはすべてのチェックボックスをオンにします。

- ・ Java — JavaはWebサイト用のプログラミング言語です。Javaをブロックするには、Javaチェックボックスをオンにします。Javaを拒否すると、このプログラミング言語で記述されたインターネットサイトにアクセスできなくなる場合があります。そのため、ルータに接続されたデバイスがJavaで作成されたWebサイトにアクセスする必要がある場合は、Javaアプレットをブロックしても安全です。一方、サイバー犯罪者は、Javaを攻撃の不可欠な要素として使用しています。これは、マルウェアに感染したWebサイトにアクセスしたときに、OSを特定し、OS固有の攻撃を開始することです。たとえば、ハッキングされたWebサイトにアクセスすると、JAR(Java Archive)ファイルがトリガーされ、その機能を実行するように求められますが、ひそかにコンピュータのOSを決定するために使用されます。
- ・ クッキー — クッキーはPCに保存されるデータで、ユーザがウェブサイトを操作する際

にインターネットサイトによって使用されます。Cookieをブロックするには、Cookiesチェックボックスにチェックマークを入れます。クッキーをブロックしたい場合は、デバイスからアクセスした際にウェブサイト以前の訪問情報を保存することはできません。この利点は、悪意のあるCookie (サードパーティのトラッキングクッキー) が保存されないことであり、これによりセキュリティリスクが生じます。

- ・ ActiveX:ActiveXは、アプリケーションの開発や、インターネットサイトで使用されるアドオンなどの小規模なプログラムの制御に使用できるMicrosoft Windowsのソフトウェアコンポーネントです。ActiveXを許可すると、参照時のエクスペリエンスが向上します。Webサイトでは、アニメーションやその他の類似プログラムを実行できます。一方、サイバー犯罪者が開発した悪意のあるActiveXソフトウェアが含まれているWebページにアクセスすると、コンピュータに損害を与える可能性があります。ActiveXをブロックするには、ActiveXチェックボックスをオンにします。ActiveXをブロックすると、ActiveXを使用する特定のインターネットサイトにアクセスして実行するときに問題が発生することがあります。

- ・ プロキシHTTPサーバへのアクセス – プロキシサーバを介して匿名でサーフィンを行い、プロキシサーバへのアクセスを拒否する場合は、「プロキシHTTPサーバへのアクセス」チェックボックスをオンにします。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。彼らは仲介者として働いているので、あなたはインターネットに直接アクセスしません。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は、ルータ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ている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。

ステップ 4 : Saveをクリックして、設定を保存します。

信頼できるドメインの追加

Web機能の1つがブロックされている場合でも、ユーザは指定された信頼できるドメインでこれらの機能を有効にすることができます。

Restrict Web Features

Block :

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.com

Add :

ステップ 1 : Don't block Java/ActiveX/Cookies/Proxy to Trusted Domainsボタンにチェックマークを入れます。これは、ユーザが「ファイアウォールの一般設定」のステップ3でWeb機能のいずれかをブロックすることを選択した場合にのみ使用できます。

Restrict Web Features

Block :

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.co

Add :

ステップ 2 : Addフィールドに、信頼できるドメインリストに追加するドメインを入力します。

Restrict Web Features

Block :

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.co

Add :

ステップ 3 : [リストに追加 (Add to List)] をクリックします。ドメインが信頼済みリストに追加されます。

ステップ 4 : Saveをクリックして、変更を保存します。

信頼されたドメインの更新

このセクションでは、信頼されたドメインを編集する方法について説明します。

The screenshot shows a web interface for managing trusted domains. At the top left, there is a label "Add :" followed by a text input field containing "www.example.com". To the right of this input field is a button labeled "Update". Below the input field is a list box containing the text "www.example.com", which is highlighted with a blue background. At the bottom right of the list box area are two buttons: "Delete" and "Add New". At the bottom left of the entire interface are two buttons: "Save" and "Cancel".

ステップ 1 : 信頼できるドメインのリストから、編集するドメインを選択します。

Add :

www.example.com

ステップ 2 : Addフィールドに、必要なドメインの更新されたドメイン名を入力します。

Add :

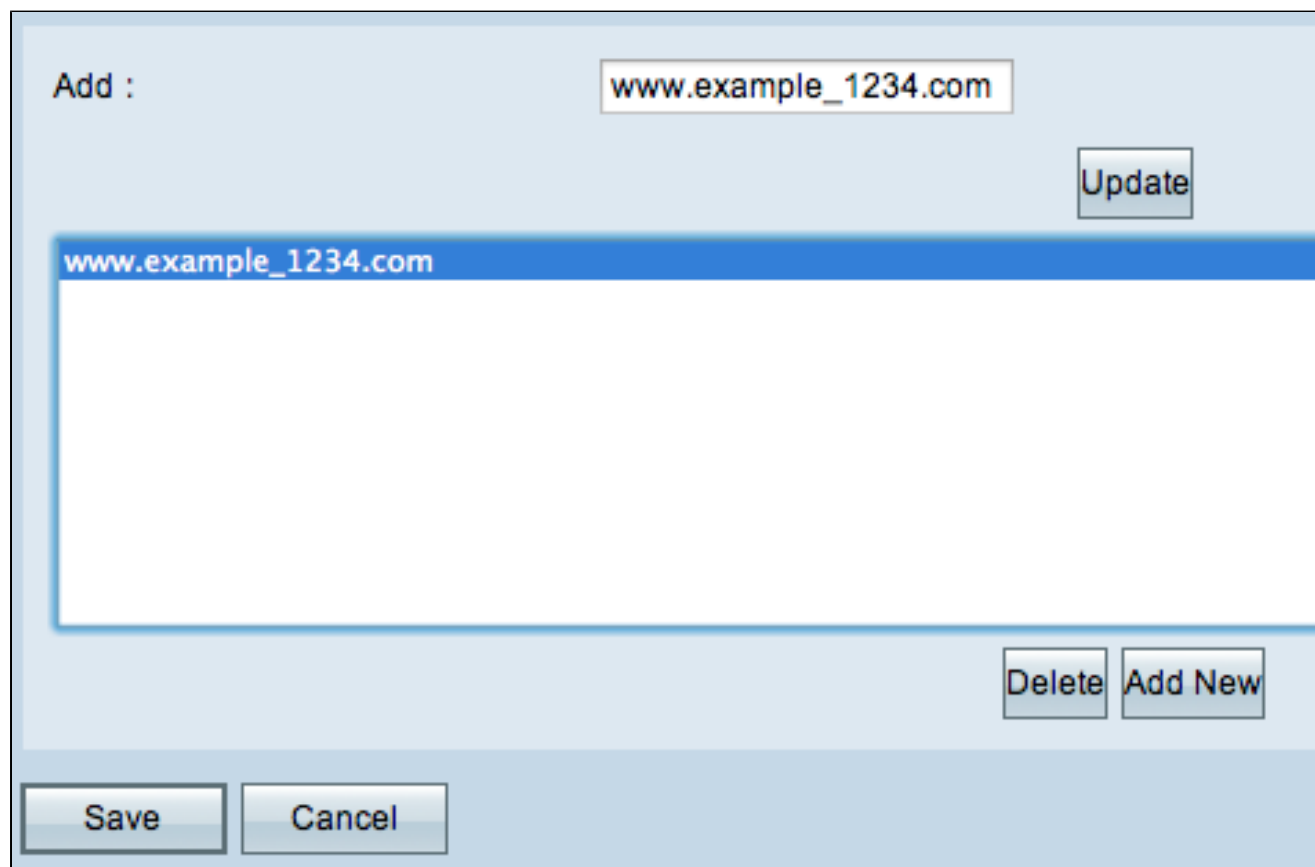
www.example.com

ステップ 3 : [Update] をクリックします。

ステップ 4 : Saveをクリックして、変更を保存します。

信頼されたドメインの削除

このセクションでは、信頼されたドメインを削除する方法について説明します。



The screenshot shows a web management interface with a light blue background. At the top left, there is a label "Add :" followed by a text input field containing "www.example_1234.com". To the right of the input field is a button labeled "Update". Below the input field is a large white rectangular area with a blue border, representing a list of domains. The text "www.example_1234.com" is visible at the top of this area. At the bottom right of the interface are two buttons: "Delete" and "Add New". At the bottom left, there are two buttons: "Save" and "Cancel".

ステップ 1 : 削除するドメインを選択します。

The screenshot shows a web management interface. At the top left, there is a label "Add :" followed by a text input field containing "www.example_1234.com". To the right of this field is an "Update" button. Below the input field is a large white area with a blue border, also containing the text "www.example_1234.com". At the bottom right of this area are two buttons: "Delete" (circled in red) and "Add New". At the bottom left of the entire interface are two buttons: "Save" and "Cancel".

ステップ 2 : [Delete] をクリックします。ドメインが削除されます。

ステップ 3 : Save をクリックして、変更を保存します。

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。