

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

## 目的

デフォルトでは、RV016、RV042、RV042G、およびRV082の組み込みファイアウォールが特定の種類のトラフィックをブロックします。ブロックされるトラフィックの種類（HTTPS、TCPおよびICMP要求、リモート管理トラフィックなど）を調整できます。ファイアウォール自体も有効または無効にできます。さらに、セキュリティの脆弱性になりうるWebサイトの特定の側面をブロックすることもできます。これらのWebサイト機能は、ブロックが解除されると、コンピュータに有害な可能性のあるデータを格納する可能性があります。

このドキュメントの目的は、RV016、RV042、RV042G、およびRV082で一般的なファイアウォール設定を行う方法を説明することです。

## 適用可能なデバイス

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

## [Software Version]

- ・ v4.2.3.06

## 一般的なファイアウォール設定の構成

ステップ 1 : Web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 :

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

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

## 一般的な機能

ステップ 1 : Firewallフィールドで、ファイアウォールをEnableまたはDisableにするオプションボタンを選択します。ファイアウォールはデフォルトで有効になっているため、無効にすることは推奨されません。ファイアウォールを無効にすると、アクセスルールとコンテンツフィルタも無効になります。

## 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 :

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

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

注：ファイアウォールを無効にする際に、デフォルトの管理者パスワードをまだ使用している場合は、パスワードの変更が必要であることを警告するメッセージが表示されます。変更を行うまでは、ファイアウォールを無効にできません。OKをクリックしてパスワードページに進むか、Cancelをクリックしてこのページを表示したままにします。

ステップ 2：SPI(Stateful Package Inspection)で、EnableまたはDisableオプションボタンを選択します。SPIはデフォルトで有効になっています。この機能を使用すると、ルータはすべてのパケットを検査してから送信し、処理することができます。これは、ファイアウォールが有効になっている場合にのみ有効にできます。

## 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

Save

Cancel

ステップ 3 : DoS(Denial of Service)フィールドで、EnableまたはDisableオプションボタンを選択します。DoSはデフォルトで有効になっています。この機能により、内部ネットワークが外部からの攻撃 ( SYNフラッディング、Smurf、LAND、Ping of Death、IPスプーフィング、リアセンブル攻撃など ) を受けないようにすることができます。これは、ファイアウォールが有効になっている場合にのみ有効にできます。

## 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

Save

Cancel

ステップ 4 : Block WAN Requestフィールドで、EnableまたはDisableオプションボタンを選択します。WAN要求のブロックはデフォルトで有効になっています。この機能を使用すると、ルータはWANからの受け入れられていないTCPおよびICMP要求をドロップし、ハッカーがWAN IPアドレスにpingを実行してルータを検出するのを防ぐことができます。これは、ファイアウォールが有効になっている場合にのみ有効にできます。

## 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 :

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

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

ステップ 5 : Remote Managementフィールドで、EnableまたはDisableオプションボタンを選択します。リモート管理はデフォルトで無効になっています。この機能を使用すると、インターネット上の任意の場所からルータのWeb設定ユーティリティに接続できます。この機能を有効にすると、リモート接続に使用するポートをPortフィールドに設定できます。デフォルト値は 443 です。

## 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 : 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

注：デフォルトの管理者パスワードを使用している場合は、パスワードの変更が必要であることを警告するメッセージが表示されます。パスワードページに進むにはOKを、このページにとどまる場合はキャンセルをクリックしてください。パスワードの変更は、権限のないユーザがデフォルトパスワードでルータにアクセスするのを防ぐために必要です。

注：リモート管理が有効になっている場合は、`http://<WAN IP address of the router>:<port>`と入力することで、任意のブラウザからWeb設定ユーティリティにアクセスできます。HTTPSが有効な場合は、代わりに`https://<WAN IP address of the router>:<port>`と入力します。

手順 6：HTTPSフィールドで、EnableまたはDisableオプションボタンを選択します。HTTPSはデフォルトで有効になっています。この機能により、セキュアなHTTPセッションが可能になります。

## 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 :

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

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

注：この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。

手順 7：Multicast Passthroughフィールドで、EnableまたはDisableオプションボタンを選択します。マルチキャストパススルーはデフォルトで無効になっています。この機能は、IPマルチキャストパケットを対応するLANデバイスにブロードキャストすることを可能にし、インターネットゲーム、ビデオ会議、およびマルチメディアアプリケーションに使用されます。



## 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

Save

Cancel

注 : RV016、RV042、RV042G、およびRV082は、IPSecトンネルを介したマルチキャストトラフィックの通過をサポートしていません。

ステップ 8 : [Save] をクリックします。

## 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 :

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

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

## Web機能

ステップ 1 : Blockフィールドで、ファイアウォールでブロックするWeb機能のチェックボックスをオンにします。一部のドメインに対してブロックされた機能を許可する場合は、これらのドメインをステップ2で例外リストに追加できます。デフォルトでは、どの機能もブロックされません。

## 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 checked="" type="checkbox"/> Java
	<input type="checkbox"/> Cookies
	<input checked="" 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	

次のオプションがあります。

- ・ Java — JavaはWebサイト用のプログラミング言語です。このチェックボックスをオンにすると、Javaアプレット（Webページに埋め込まれていても、Webブラウザの外部で実行される小さなプログラム）はブロックされますが、この機能を使用するWebサイトが正しく動作しなくなる可能性があります。
- ・ クッキー：クッキーとは、WebサイトがユーザのPCにローカルに保存するデータのことです。クッキーをブロックすると、クッキーに依存するWebサイトが正しく動作しなくなる可能性があります。
- ・ ActiveX:ActiveXは、Microsoftによって開発されたソフトウェア・フレームワークです。このフレームワークは、Webページの特定の部分を実行するために使用できます。このチェックボックスをオンにすると、これらのコンポーネントはブロックされますが、ActiveXを使用するWebサイトが正しく動作しなくなる可能性があります。

- ・ HTTPプロキシサーバへのアクセス – HTTPプロキシサーバへのアクセスをブロックする場合は、このチェックボックスをオンにします。WANプロキシサーバを使用すると、ルータのセキュリティが低下する可能性があります。

ステップ 2 : Don't block Java/ActiveX/Cookies/Proxy to Trusted Domainsチェックボックスにチェックマークを入れて、信頼できるドメインリストを開きます。このリストで、ブロックされたWeb機能が許可されているドメインを追加または削除できます。このフィールドはデフォルトでオフになっており、前のボックスをオンにしてフィーチャをブロックした場合にのみ使用できます。オフにすると、すべてのWebサイトで機能がブロックされます。

The screenshot shows the 'General' configuration page. The 'Firewall' section has several options: Firewall (Enable selected), SPI (Stateful Packet Inspection) (Enable selected), DoS (Denial of Service) (Enable selected), Block WAN Request (Enable selected), Remote Management (Disable selected, Port: 443), HTTPS (Enable selected), and Multicast Passthrough (Disable selected). The 'Restrict Web Features' section has a 'Block' section with checkboxes for Java (checked), Cookies (unchecked), ActiveX (checked), and Access to HTTP Proxy Servers (unchecked). A red box highlights the checkbox for 'Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.com', which is currently unchecked. At the bottom are 'Save' and 'Cancel' buttons.

ステップ3: ( オプション ) Don't block Java/ActiveX/Cookies/Proxy to Trusted Domainsチェックボックスにチェックマークを入れると、信頼できるドメインのリストが表示されます。リストにドメインを追加するには、Addフィールドにドメインを入力し、Add to Listをクリックします。既存のドメインを変更する場合は、リストでそのドメインをクリックし、Addフィールドで編集して、Updateをクリックします。リストからドメインを削除するには、リストでそのドメインをクリックし、Deleteをクリックします。

**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.com

Add :

www.cisco.com  
www.example.com

ステップ 4 : [Save] をクリックします。

## General

Firewall :  Enable  Disable

SPI (Stateful Packet Inspection) :  Enable  Disable

DoS (Denial of Service) :  Enable  Disable

Block WAN Request :  Enable  Disable

Remote Management :  Enable  Disable

Port :

HTTPS :  Enable  Disable

Multicast Passthrough :  Enable  Disable

### 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

Save

Cancel

## 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。