

# RV016、RV082、RV042、およびRV042G VPNルータでのウィザードによるアクセスルールの設定

## 目的

アクセスルールは、ネットワークのセキュリティを確保するために、トラフィックがルータのファイアウォールを通過してネットワーク内に入ることを許可するかどうかを決定するために使用されます。アクセスルールは、ネットワークへのアクセスを許可または拒否するためのさまざまな基準に基づいて設定されます。アクセスルールは、アクセスルールをルータに適用する必要がある時間に従ってスケジュールされます。

この記事では、RV016、RV082、RV042、およびRV042G VPNルータでウィザードを使用してアクセスルールを設定する方法について説明します。

注：ファイアウォールを介してアクセスルールを設定できます。ファイアウォールによるアクセスルールの設定方法の詳細については、『IPv4アクセスルール用のRV016、RV082、RV042、およびRV042G VPNルータでのIPv4アクセスルールの設定』および『IPv6アクセスルール用のRV042、RV016、およびRV042G VPNルータ』を参照してください。v6アクセスルール。ファイアウォールを使用してアクセスルールをスケジュールすることもできます。ファイアウォールによるアクセスルールのスケジュール方法の詳細については、『RV016、RV082、RV042およびRV042Gでのアクセスルールのスケジュール』を参照してください。

## 適用可能なデバイス

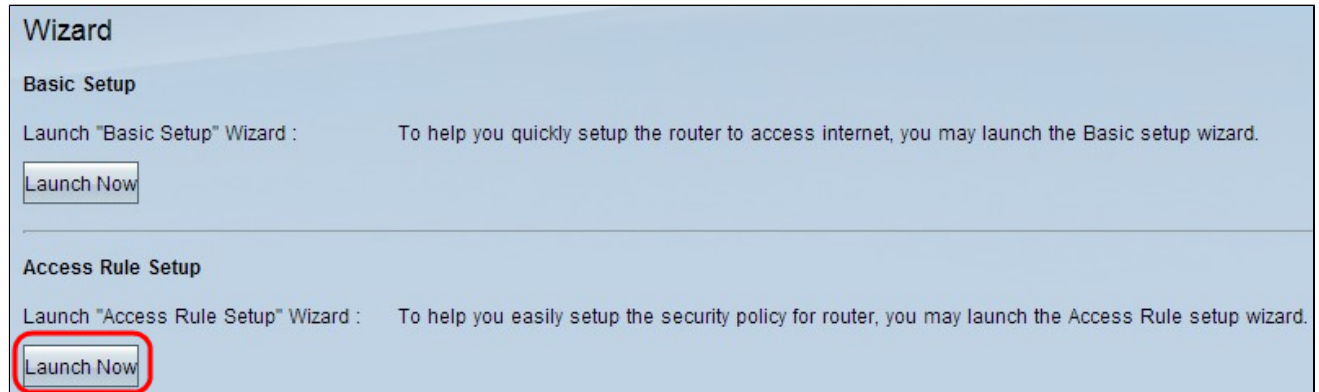
- ・ RV042
- ・ RV042G
- ・ RV082
- ・ RV016

## [Software Version]

- ・ v4.2.1.02

# アクセスルールの設定

ステップ 1 : Router Configuration Utilityを使用して、Wizardを選択します。Wizardページが開きます。



ステップ 2 : Access Rule SetupセクションのLaunch Nowをクリックして、Access Rule Installation Wizardを設定します。このページでは、ルータのアクセスルールとデフォルトルールについて説明します。Welcome to the Access Rules Installation Wizardウィンドウが開きます。

## Welcome to the Access Rules Installation Wizard

Network Access Rules evaluate network traffic's Source IP address, Destination IP address, and IP protocol type to decide if the IP traffic is allowed to pass through the firewall. Custom rules take precedence, and may override RV042G's default stateful packet inspection.

The ability to define Network Access Rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting Network Access Rules.

RV042G has the following default rules :

- All traffic from the LAN to the WAN is allowed.
- All traffic from the WAN to the LAN is denied.
- All traffic from the LAN to the DMZ is allowed.
- All traffic from the DMZ to the LAN is denied.
- All traffic from the WAN to the DMZ is allowed.
- All traffic from the DMZ to the WAN is allowed.

Custom rules can be created to override the RV042G default rules.

Back

Next

Cancel

ステップ 3 : Nextをクリックしてセットアップを続行します。

**Action** Select the Action.

Service

Log

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Select **Allow** or **Deny** depending on the intent of the rule. For example, to configure the Router to allow all FTP traffic access from the LAN to the Internet. Thus select Allow. Or, to restrict all FTP traffic access from the LAN to the Internet. Thus select Deny.

Action:

Back Next Cancel

ステップ 4 : Actionドロップダウンリストから適切なオプションボタンを選択して、LAN/WANからインターネットへのFTPトラフィックを許可または制限します。

- ・ Allow : すべてのFTPトラフィックがLAN/WANからインターネットにアクセスすることを許可します。
- ・ Deny:LAN/WANからインターネットにアクセスするすべてのFTPトラフィックを制限します。

ステップ 5 : Nextをクリックしてセットアップを続行します。

✓ Action      Select the Service.

**Service**      Select the service that will be allowed or denied from the Service menu.

Log

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Service: All Traffic [TCP&UDP/1~65535]    ▼  
All Traffic [TCP&UDP/1~65535]    ▲  
DNS [UDP/53~53]  
FTP [TCP/21~21]  
HTTP [TCP/80~80]  
HTTP Secondary [TCP/8080~8080]  
HTTPS [TCP/443~443]  
HTTPS Secondary [TCP/8443~8443]  
TFTP [UDP/69~69]  
IMAP [TCP/143~143]  
NNTP [TCP/119~119]  
POP3 [TCP/110~110]  
SNMP [UDP/161~161]  
SMTP [TCP/25~25]  
TELNET [TCP/23~23]  
TELNET Secondary [TCP/8023~8023]  
TELNET SSL [TCP/992~992]  
DHCP [UDP/67~67]  
L2TP [UDP/1701~1701]  
PPTP [TCP/1723~1723]  
IPSec [UDP/500~500]    ▼

Back      Next      Cancel

手順 6 : Service ドロップダウンリストから、許可または拒否する必要がある適切なサービスを選択します。

手順 7 : Next をクリックしてセットアップを続行します。

✓ Action      Select the Log.

✓ Service      You can select **Log packets match this rule** or **Not log**.

**Log**

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Log: Log packets match this rule ▼  
Log packets match this rule  
Not log

Back      Next      Cancel

ステップ 8 : Log ドロップダウンリストから適切な Log オプションを選択します。

- ・ ログパケットがこのアクセスルールに一致する : ルータが、選択されたサービスのログトラッキングを保持できるようにします。
- ・ Not Log : ルータがログの追跡を継続できないようにします。

ステップ 9 : [Next] をクリックして次に進みます。

✓ Action      Select the Source Interface.

✓ Service      Select the source, either WAN, LAN, DMZ or Any from the Source Interface menu. For example, allow all FTP traffic access from the LAN to the Internet. Thus select the LAN as source.

✓ Log

**Source Interface**

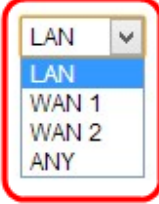
Source IP

Destination IP

Schedule

Summary

Finish

Interface: 


Back      Next      Cancel

ステップ10:Interfaceドロップダウンリストから適切な送信元インターフェイスを選択します。

- ・ LAN : 送信元インターフェイスはローカルエリアネットワークです。アクセスルールはLANトラフィックにのみ影響します。
- ・ WAN 1 : 送信元インターフェイスはワイドエリアネットワーク1です。アクセスルールはWAN 1トラフィックだけに影響します。
- ・ WAN 2 : 送信元インターフェイスはワイドエリアネットワーク2です。アクセスルールはWAN 2トラフィックにのみ影響します。
- ・ Any : 送信元インターフェイスには、任意のネットワークを指定できます。アクセスルールは、すべてのトラフィックに影響します。

ステップ 11[Next] をクリックして次に進みます。

Action Select the Source IP type and enter the IP address.  
 Service  
 Log For example, allow all users on LAN side to access the Internet. Thus select Any. Allow certain user(s) on LAN side to access the Internet. Thus select Single or Range and enter the IP address.  
 Source Interface  
**Source IP**  
 Destination IP  
 Schedule  
 Summary  
 Finish




ステップ 12 Source IP ドロップダウンリストから、アクセスルールを適用する適切な送信元 IP アドレスまたは IP アドレスの範囲を選択します。

- ・ Any : 任意の IP アドレスを持つ任意のユーザがインターネットにアクセスできます。
- ・ Single: 1つの IP アドレスを持つ 1人のユーザだけがインターネットにアクセスできます。Single を選択した場合は、特定の IP アドレスを入力する必要があります。
- ・ 範囲 : IP アドレスの範囲を持つユーザだけがインターネットにアクセスできます。Range を選択した場合は、開始 IP アドレスと終了 IP アドレスを入力する必要があります。

ステップ 13 下にスクロールして Next をクリックし、セットアップを続行します。

Action Select the Destination IP type and enter the IP address.  
 Service Select the destination, either Any, Single or Range \* from the Destination IP pull-down menu. For example, allows Internet can access the DMZ port, thus select Single or Range and enter the IP address of DMZ port.  
 Log  
 Source Interface  
 Source IP  
**Destination IP**  
 Schedule  
 Summary  
 Finish



ステップ 14 : Destination IP ドロップダウンリストから、アクセスルールに適切な宛先 IP アドレスまたは IP アドレスの範囲を選択します。

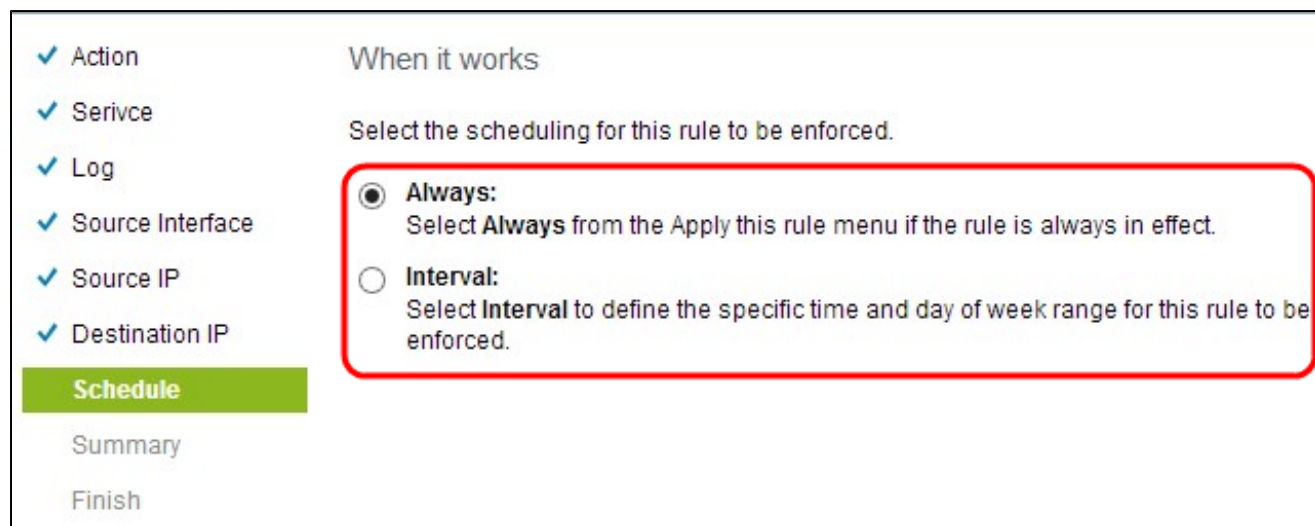
- ・ Any : 宛先インターフェイスは任意の IP アドレスを持つことができます。



・ Single : 宛先インターフェイスは、特定の単一IPアドレスにすることができます。Singleを選択した場合は、特定の単一IPアドレスを入力する必要があります。

・ Range : 宛先インターフェイスは、特定の範囲の任意のIPアドレスにすることができます。Rangeを選択した場合は、開始IPアドレスと終了IPアドレスを入力する必要があります。

ステップ 15 : 下にスクロールしてNextをクリックし、セットアップを続行します。



When it works

Select the scheduling for this rule to be enforced.

- Always:**  
Select **Always** from the Apply this rule menu if the rule is always in effect.
- Interval:**  
Select **Interval** to define the specific time and day of week range for this rule to be enforced.

Left sidebar tabs: Action, Service, Log, Source Interface, Source IP, Destination IP, **Schedule**, Summary, Finish

ステップ 16 : 適切なオプションボタンをクリックして、ルータにアクセスルールを適用する時刻を選択します。

・ Always : アクセスルールは常にルータに適用されます。このオプションを選択する場合は、ステップ17からステップ19までをスキップしてください。デフォルトはAlwaysです。

・ Interval : アクセスルールは、設定された時間に応じて特定の時間だけ適用されます。このオプションを選択した場合は、アクセスルールを適用する時間間隔を入力する必要があります。

✓ Action	Enter the Scheduling
✓ Service	<b>Time Setting</b>
✓ Log	Enter the time of day (in 24-hour format) to begin and end enforcement.
✓ Source Interface	From: <input type="text" value="03:10"/> (hh:mm) To: <input type="text" value="10:10"/> (hh:mm)
✓ Source IP	
✓ Destination IP	
<b>Schedule</b>	<b>Date Setting</b>
Summary	Enter the day of week to begin and end enforcement.
Finish	<input type="checkbox"/> Everyday <input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat

ステップ 17 : アクセスリストのスケジュールを適用する開始時刻をFromフィールドに入力します。時刻の形式はhh: mmです。

ステップ 18 : アクセスリストのスケジュールを適用する時間を[宛先]フィールドに入力します。時刻の形式はhh: mmです。

ステップ 19 : アクセスリストのスケジュールを適用する場合は、特定のチェックボックスをオンにします。

ステップ 20 : 下にスクロールしてNextをクリックし、セットアップを続行します。アクセスルールの詳細情報を含むサマリーウィンドウが開きます。

✓ Action	Summary	
✓ Service	<b>Action:</b>	Allow
✓ Log	<b>Service:</b>	All Traffic [TCP&UDP/1~65535]
✓ Source Interface	<b>Log:</b>	Log packets match this rule
✓ Source IP	<b>Source Interface:</b>	LAN
✓ Destination IP	<b>Source IP:</b>	Any
✓ Schedule	<b>Destination IP:</b>	Any
<b>Summary</b>	<b>Schedule:</b>	From 03:10 to 10:10 , Mon , Tue , Fri
Finish		

ステップ 21 : 下にスクロールし、Installをクリックしてセットアップをインストールします。  
。

ステップ 22 : OKをクリックして設定を保存し、ウィザードページに戻ります。

## 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。