

# RV32x VPNルータシリーズのアクセスルールセットアップウィザード

## 目的

アクセスルール設定ウィザードは、RV32xルータの初期設定を簡単にガイド付きで設定できます。デバイスを設定するための手順をユーザに説明します。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基づいてスケジュールされます。この記事では、ファイアウォールを介してネットワークに入ることを許可するトラフィックを判別するために使用されるアクセスルールセットアップウィザードの概要と説明を示します。

## 該当するデバイス

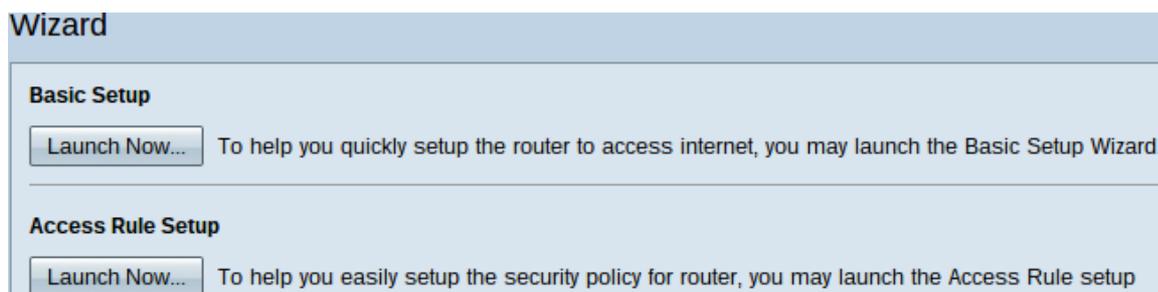
- ・ RV320デュアルWAN VPNルータ
- ・ RV325ギガビットデュアルWAN VPNルータ

## [Software Version]

- ・ v1.1.0.09

## アクセスルール設定ウィザード

ステップ1：ルータ設定ユーティリティにログインし、[Wizard]を選択します。[ウィザード]ページが開きます。



ステップ2:[Access Rule Setup]領域の下にある[Launch Now]ボタンをクリックして、アクセスルールのセットアップウィザードを開始します。[アクセスルールのセットアップ]インストールウィザードダイアログボックスが表示されます。

## 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 these rules. RV320'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 access to the Internet. Use extreme caution when creating or deleting Network Access Rules.

RV320 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 RV320 default rules.



Back

Next

Cancel

ステップ3:[次へ]をクリックして、ウィザードに進みます。

## アクション

### 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 to the Internet from the LAN, select Allow. Or, to restrict all FTP traffic access Internet from the LAN, select Deny.

Action:

Back

Next

Cancel

ステップ1:[Action (アクション)]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、設定しようとしているルールを許可または制限します。アクセスルールは、特定のサービスまたはデバイスからのトラフィックアクセスを許可または拒否することによって、

サブネットワークへのアクセスを制限します。

- ・ Allow : すべてのトラフィックを許可します。
- ・ Deny : すべてのトラフィックを制限します。

ステップ2 : ウィザードを続行するには、[次へ]をクリックします。

## サービス

✓ Action	Select the Service.
<b>Service</b>	Select the service that will be allowed or denied from the Service menu.
Log	
Source Interface	Service: <input type="text" value="POP3 [TCP/110~110]"/>
Source IP	
Destination IP	
Schedule	
Summary	
Finish	

<input type="button" value="Back"/>	<input type="button" value="Next"/>	<input type="button" value="Cancel"/>
-------------------------------------	-------------------------------------	---------------------------------------

ステップ1:[Service ( サービス )]ドロップダウンリストから、許可または制限する必要がある適切なサービスを選択します。

注 : すべてのトラフィックを許可するには、アクションが[許可]に設定されている場合は、サービスのドロップダウンリストから[すべてのトラフィック[TCP&UDP/1 ~ 65535]]を選択します。このリストには、フィルタ処理するサービスのすべてのタイプが含まれています。

ステップ2:[Next]をクリックし、セットアップを続行します。

log

✓ Action

Select the Log.

✓ Service

You can select **Log packets matching this rule** or **Not log**.

Log

Log:

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Back

Next

Cancel

ステップ1:[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。logオプションは、アクセスルールの設定に対応するトラフィックのログをデバイスが保持するかどうかを決定します。

- ・ ログパケットがこのアクセスルールに一致する：選択されたサービスのログトラッキングをルータが維持できるようにします。
- ・ Not Log：ログトラッキングを維持するためにルータを無効にします。

ステップ2:[Next]をクリックし、セットアップを続行します。

## 送信元インターフェイス

✓ Action                      Select the Source Interface.

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

✓ Log

**Source Interface**            Interface:

Source IP

Destination IP

Schedule

Summary

Finish

ステップ1:[Interface]ドロップダウンリストをクリックし、適切な送信元インターフェイスを選択します。このインターフェイスでは、アクセスルールが適用されます。

- ・ LAN : 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 : アクセスルールはWAN 1トラフィックにのみ影響します。
- ・ WAN 2 : 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 : アクセスルールは、デバイスのいずれかのインターフェイス内のすべてのトラフィックに影響します。

ステップ2:[Next]をクリックし、セットアップを続行します。

## 送信元 IP

✓ Action Select the Source IP type and enter the IP address.

✓ Service For example, to allow all users on LAN side to access the Internet, select Any. To allow certain users on LAN side to access the Internet, select Single or Range and enter the IP address.

✓ Log

✓ Source Interface

**Source IP**

Destination IP

Schedule

Summary

Finish

ステップ1：使用可能な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タイプを選択します。

- ・ Any：デバイスのネットワークの任意のIPアドレスに、ルールが適用されています。

Select the Source IP type and enter the IP address.

For example, to allow all users on LAN side to access the Internet, select Any. To allow certain users on LAN side to access the Internet, select Single or Range and enter the IP address.

- ・ Single：デバイスのネットワークの指定された単一のIPアドレスにのみ、ルールが適用されます。目的のIPアドレスを入力します。

Select the Source IP type and enter the IP address.

For example, to allow all users on LAN side to access the Internet, select Any. To allow certain users on LAN side to access the Internet, select Single or Range and enter the IP address.

To

- ・ 範囲：ネットワーク上の指定された範囲のIPアドレスにのみ、ルールが適用されます。[範囲]を選択した場合は、範囲の開始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2:[Next]をクリックし、セットアップを続行します。

## 宛先 IP

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.  
 Log For example, to allow access to the DMZ port from the Internet, select Single or Range and enter the IP address of DMZ port.  
 Source Interface  
 Source IP

**Destination IP**

Schedule

Summary

Finish

ステップ1：使用可能な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宛先IPタイプを選択します。

- ・ Any：すべての宛先IPアドレスにルールが適用されます。

Select the Destination IP type and enter the IP address.

Select the destination, either Any, Single or Range \* from the Destination IP pull-down menu.  
For example, to allow access to the DMZ port from the Internet, select Single or Range and enter the IP address of DMZ port.

- ・ Single：ルールが適用された単一の指定IPアドレスのみ。目的のIPアドレスを入力します。

Select the Destination IP type and enter the IP address.

Select the destination, either Any, Single or Range \* from the Destination IP pull-down menu.  
For example, to allow access to the DMZ port from the Internet, select Single or Range and enter the IP address of DMZ port.

To

- ・ 範囲：デバイスのネットワーク外に出る指定された範囲のIPアドレスにのみ、ルールが適用されます。[範囲]を選択した場合は、範囲の開始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2:[Next]をクリックし、セットアップを続行します。

## Schedule

- ✓ Action
- ✓ Service
- ✓ Log
- ✓ Source Interface
- ✓ Source IP
- ✓ Destination IP

### Schedule

Summary

Finish

### 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.

Back

Next

Cancel

ステップ1：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でアクティブです。このオプションを選択した場合は、ステップ5に進みます。これがデフォルトです。
- ・ **間隔** : アクセスルールは特定の時間アクティブです。このオプションを選択する場合は、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

✓ Log

✓ Source Interface

✓ Source IP

✓ Destination IP

**Schedule**

Summary

Finish

**Time Setting**

Enter the time of day (in 24-hour format) to begin and end enforcement.

From:  (hh:mm)

To:  (hh:mm)

---

**Date Setting**

Enter the day of week to begin and end enforcement.

Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

ステップ2 : アクセスリストを適用する時刻を[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3:[To]フィールドにアクセスリストを適用するまでの時間を入力します。時刻の形式はhh:mmです。

ステップ4 : アクセスリストを適用する特定の日のチェックボックスをオンにします。

ステップ5:[Next]をクリックし、セットアップを続行します。

## 要約

✓ Action	Summary
✓ Service	Please review the following settings and ensure the data is correct.
✓ Log	<b>Action:</b> Deny
✓ Source Interface	<b>Service:</b> All Traffic [TCP&UDP/1~65535]
✓ Source IP	<b>Log:</b> Not log
✓ Destination IP	<b>Source Interface:</b> WAN 2
✓ Schedule	<b>Source IP:</b> 192.0.2.4
<b>Summary</b>	<b>Destination IP:</b> Any
Finish	<b>Schedule :</b> From 04:30 To 17:14 , Sun , Tue

注 : [Summary]ページには、アクセスセットアップウィザードによってRV320で設定されたすべての設定の全体像が表示されます。

ステップ1:[Submit]をクリックし、ウィザード構成に対する変更を送信します。

## 終了

✓ Action	Device Setup Complete
✓ Service	<b>Access Rules have been successfully configured.</b>
✓ Log	
✓ Source Interface	
✓ Source IP	
✓ Destination IP	
✓ Schedule	
✓ Summary	
<b>Finish</b>	

ステップ1:[Finish]をクリックし、アクセスルールのセットアップウィザードを終了します。