

RV320およびRV325 VPNルータのアクセスルール設定

目的

アクセスコントロールリスト(ACL)は、特定のユーザとの間で送受信されるトラフィックをブロックまたは許可するリストです。アクセスルールは、常に有効になるように、または定義されたスケジュールに基づいて設定できます。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、ルータのファイアウォールを介してトラフィックがネットワークに入ることを許可するか、ネットワークのセキュリティを確保するかを決定するために使用するアクセスルール設定ウィザードの概要と説明します。

該当するデバイス | ファームウェアのバージョン

- RV320デュアルWAN VPNルータ | V 1.1.0.09 (最新の[ダウンロード](#))
- RV325ギガビットデュアルWAN VPNルータ | V 1.1.0.09 (最新の[ダウンロード](#))

アクセスルールの設定

ステップ1: Web構成ユーティリティにログインし、[Firewall] > [Access Rules]を選択します。「アクセス規則」ページが開きます。

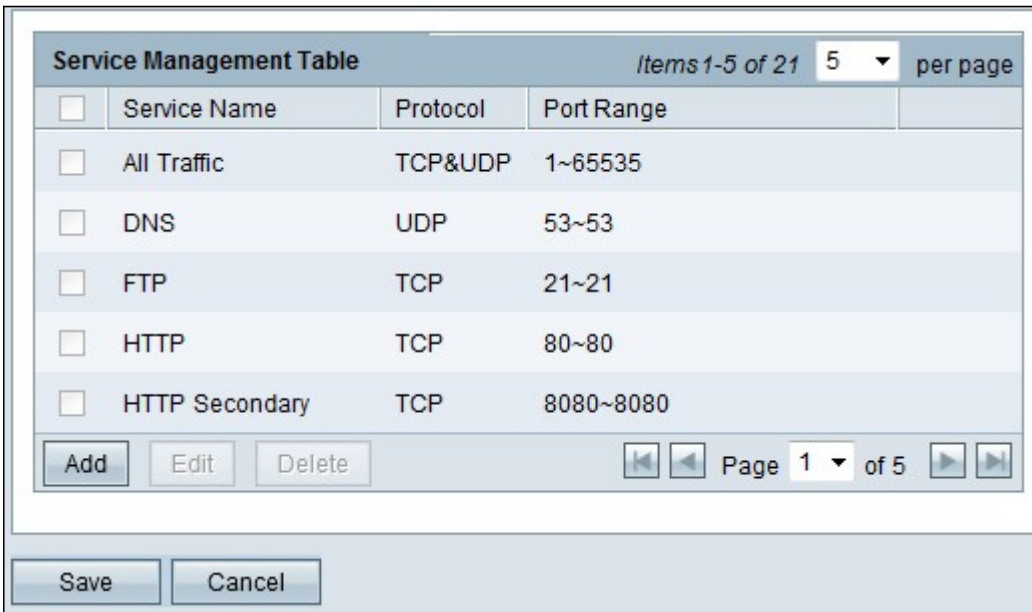
Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

アクセスルールテーブルには、次の情報が含まれます。

- [Priority] : アクセスルールの優先度を表示します
- [Enable] : アクセスルールが有効か無効かを表示します
- [Action] : アクセスルールが許可または拒否されていることを示します。
- Service : サービスのタイプを表示します。
- SourceInterface : アクセスルールが適用されているインターフェイスを表示します。
- Source : 送信元デバイスのIPアドレスを表示します
- Destination : 宛先デバイスのIPアドレスを表示します
- Time : アクセスルールが適用される時間を表示します
- [Day] : アクセスルールが適用された1週間の間に表示されます

Service Management

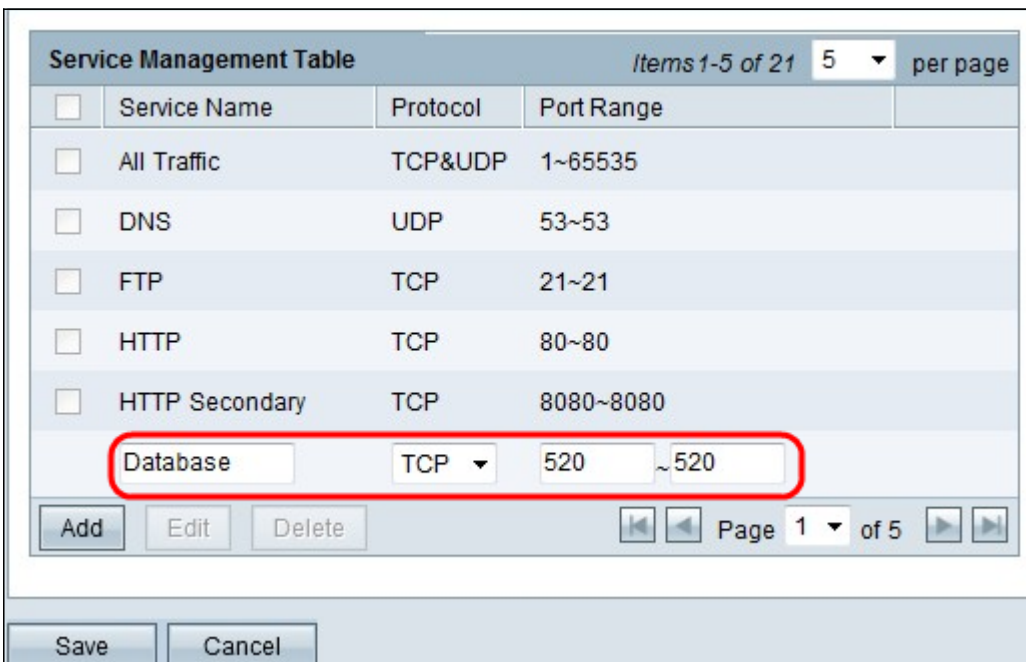
ステップ1：新しいサービスを追加するには、[サービス管理]をクリックします。「サービス管理」(Service Management)テーブルページが開きます。



The screenshot shows a web interface titled "Service Management Table" with a table of services. The table has columns for "Service Name", "Protocol", and "Port Range". Below the table are "Add", "Edit", and "Delete" buttons, and a pagination control showing "Page 1 of 5".

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080

ステップ2：新しいサービスを追加するには、[追加]をクリックします。



The screenshot shows the same "Service Management Table" interface, but with a new service entry "Database" added at the bottom. The "Database" entry is highlighted with a red rectangle. The "Add" button is also visible.

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080
<input type="checkbox"/>	Database	TCP	520 ~ 520

ステップ3：次のフィールドを設定します。

- [Service Name]：要件に基づいて、サービスの名前を指定します
- [Protocol]：サービスのプロトコルTCPまたはUDPを選択します
- [ポート範囲(Port Range)]：要件に基づいてポート番号の範囲を入力します。ポート番号は範囲内(1 ~ 65536)である必要があります。

ステップ4:[Save]をクリックして変更を保存します

IPv4のアクセスルール設定

Access Rules									
Access Rules Table Items 1-5 of 5 5 per page									
	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Page 1 of 1

ステップ1:[Add]をクリックして、新しいアクセスルールを設定します。[Edit Access Rules]ウィンドウが表示されます。

Edit Access Rules

Services

Action:

Service:
 [TCP&UDP/1~65535]

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

ステップ2:[Action]ドロップダウンリストから適切なオプションを選択し、設定しようとしているルールのトラフィックを許可または制限します。アクセスルールは、さまざまな値に基づいて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。

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on: Mon Tue Wed Thu Fri Sat

ステップ3:[Service]ドロップダウンリストから、フィルタリングする必要がある適切なサービスを選択します。

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

ステップ4:[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。

- このアクセスルールに一致するログパケット：ルータは、選択されたサービスを追跡するログを保持します。
- Not Log：ルータはアクセスルールのログを保持しません。

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

ステップ5:[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。
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、デバイスの任意のインターフェイスのすべてのトラフィックに影響します。

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

ステップ6:[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、ルールが適用されます。
- [Single] : デバイスのネットワーク上で指定された1つのIPアドレスにのみ、ルールが適用されます。隣接するフィールドに目的のIPアドレスを入力します。
- [範囲(Range)] : デバイスのネットワーク上で指定された範囲の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、範囲の最初と最後のIPアドレスを隣接するフィールドに入力する必要があります。

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

ステップ7：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：任意の宛先IPアドレスにルールが適用されます。
- Single：ルールが適用されるのは、指定された1つのIPアドレスだけです。隣接するフィールドに目的のIPアドレスを入力します。
- [範囲(Range)]：デバイスのネットワーク外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、範囲の最初と最後のIPアドレスを隣接するフィールドに入力する必要があります。

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

タイムサーバ:デフォルトでは、時間は[Always]に設定されています。アクセスルールを特定の時刻または日付に適用する場合は、ステップ8からステップ11に進みます。適用しない場合は、ス

トップ12に進みます。

ステップ8：ドロップダウンリストから[Interval]を選択します。アクセスルールは特定の時間アクティブです。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。

Scheduling

Time: Interval ▼

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

ステップ9:[From]フィールドに、アクセスリストの適用を開始する時刻を入力します。時刻の形式はhh:mmです。

ステップ10:[To]フィールドに、アクセスリストを適用しない時刻を入力します。時刻の形式はhh:mmです。

Scheduling

Time: Interval ▼

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

ステップ11：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。

手順 12： [Save] をクリックして変更内容を保存します。

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 6 5 ▼

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input checked="" type="radio"/>	1 ▼	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management... Page 1 of 2

ステップ13: (オプション) デフォルトのルールを復元する場合は、「デフォルトのルールに復元」をクリックします。ユーザが設定したすべてのアクセスルールが失われます。

IPv6のアクセスルール設定

The screenshot shows the 'Access Rules' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6'. The 'IPv6' tab is selected and highlighted with a red circle. Below the tabs is the 'Access Rules Table' with columns: Priority, Enable, Action, Service, SourceInterface, Source, Destination, Time, and Day. The table contains five rows of rules. At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Restore to Default Rules', and 'Service Management...'. The page number 'Page 1 of 1' is visible at the bottom right.

ステップ1:[IPv6]タブをクリックして、IPv6アクセスルールを設定します。

This screenshot is identical to the previous one, but the 'Add' button at the bottom left of the 'Access Rules Table' is highlighted with a red circle.

ステップ2:[Add]をクリックして、新しいIPv6アクセスルールを追加します。[Edit Access Rules]ウィンドウが表示されます。

The screenshot shows the 'Edit Access Rules' dialog box. It has several fields: 'Action' (set to 'Allow'), 'Service' (set to '[TCP&UDP/1~65535]'), 'Log' (set to 'No Log'), 'Source Interface' (set to 'LAN'), 'Source IP / Prefix Length' (set to 'ANY'), and 'Destination IP / Prefix Length' (set to 'ANY'). The 'Action' dropdown menu is open, and the 'Allow' option is highlighted with a red circle. At the bottom, there are buttons for 'Save', 'Cancel', and 'Back'.

ステップ3:[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を選択し、設定する必要があ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、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。

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Save Cancel

- 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]
- Ping [ICMP/255~255]
- data [TCP/520~521]

ステップ4:[Service]ドロップダウンリストから、フィルタリング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。

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: No Log

Source Interface: Enabled

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

ステップ5:[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。

- [有効(Enabled)] : 選択したサービスのログトラッキングをルータが保持できるようにします。
- [ログなし(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。

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: LAN

Destination IP / Prefix Length: ANY

Save Cancel Back

ステップ6:[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、デバイスの任意のインターフェイスのすべてのトラフィックに影響します。

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

ステップ7:[Source IP/Prefix Length]ドロップダウンリストから、アクセスルールが適用される適切な送信元IPタイプを選択します。

- ANY : デバイスのネットワークから受信されたパケットには、ルールが適用されます。

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- [Single] : デバイスのネットワーク内で指定された1つのIPアドレスにのみ、ルールが適用されます。隣接フィールドに目的のIPv6アドレスを入力します。

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- サブネット : サブネットのIPアドレスにのみ、ルールが適用されます。隣接するフィールドに、IPv6ネットワークアドレスと目的のサブネットのプレフィクス長を入力します。

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

ANY
Single
Subnet

Save Cancel Back

ステップ8:[Destination IP / Prefix Length]ドロップダウンリストから、アクセスルールが適用される適切な宛先IPタイプを選択します。

- Any : 任意の宛先IPアドレスにルールが適用されます。
- [Single] : デバイスのネットワーク上で指定された1つのIPアドレスにのみ、ルールが適用されます。目的のIPv6アドレスを入力します。
- サブネット : サブネットのIPアドレスにのみ、ルールが適用されます。隣接するフィールドに、IPv6ネットワークアドレスと目的のサブネットのプレフィクス長を入力します。

ステップ9:[Save]をクリックし、変更を有効にします。

この記事に関連するビデオを表示...

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)