

RV016、RV042、RV042G、およびRV082 VPNルータでのIPv6アクセスルールの設定

目的

アクセスルールは、どのトラフィックがファイアウォールを通過できるかをルータが判断するのに役立ちます。これにより、ルータのセキュリティが向上します。

この記事では、RV016、RV042、RV042G、およびRV082 VPNルータでIPv6アクセスルールを追加する方法について説明します。

適用可能なデバイス

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

[Software Version]

- ・ v4.2.1.02

IPv6アクセスルールの設定

IPv6モードの有効化

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

Network

Host Name : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

LAN Setting

MAC Address : 54:75:D0:F7:FB:52

Device IP Address :

Subnet Mask : ▼

Multiple Subnet : Enable

ステップ 2 : Dual-Stack IP オプションボタンをクリックします。これにより、IPv4 と IPv6 を同時に実行できます。IPv6 通信が可能な場合は、それが優先される通信です。

IPv6 アクセスルールの設定

ステップ 1 : Web 設定ユーティリティにログインし、Firewall > Access Rules の順に選択します。アクセスルールページが開きます。

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	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		

Add Restore to Default Rules Page 1 of 1

ステップ 2 : [IPv6]タブをクリックします。これにより、IPv6 Access Rulesページが開きます。

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	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	

Add Restore to Default Rules Page 1 of 1

ステップ 3 : Addをクリックして、アクセスルールを追加します。IPv6のアクセスルールを設定するためのアクセスルールページが表示されます。

Access Rules

Services

Action : Allow

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

Service Management

Log : Log packets match this rule

Source Interface : LAN

Source IP / Prefix Length: Single / 128

Destination IP / Prefix Length: Single / 128

Save Cancel

ステップ 4 : トラフィックを許可する場合は、ActionドロップダウンリストからAllowを選択

します。Denyを選択して、トラフィックを拒否します。

ステップ 5 : Service ドロップダウンリストから適切なサービスを選択します。

タイムサーバー : 目的のサービスが使用可能な場合は、ステップ12に進みます。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: /

Destination IP / Prefix Length: /

手順 6 : 適切なサービスを使用できない場合は、Service Managementをクリックします。Service Managementウィンドウが表示されます。

Service Name :

Protocol :

TCP ▾

Port Range :

to

Add to list

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]

Delete

Add New

OK

Cancel

Close

Service Name :

Protocol :

Port Range : to

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]

手順 7 : Service Nameフィールドに新しいサービスの名前を入力します。

Service Name :

Protocol : TCP ▼

Port Range : to

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]

ステップ 8 : Protocol ドロップダウンリストから適切なプロトコルタイプを選択します。

- ・ TCP (Transmission Control Protocol ; 伝送制御プロトコル) : 保証された配信を必要とするアプリケーションで使用されるトランスポート層プロトコル。

- ・ UDP(User Datagram Protocol) : データグラムソケットを使用して、ホストとホスト間の通信を確立します。UDP配信は保証されません。
- ・ IPv6 (インターネットプロトコルバージョン6) : ルーティングアドレスで指定されたネットワークを介してルーティングされるパケット内のホスト間でインターネットトラフィックを転送します。

Service Name :

Protocol :

Port Range : to

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]

ステップ 9 : Port Rangeフィールドにポート範囲を入力します。この範囲は、上記の手順で選択したプロトコルによって異なります。

ステップ 10 : [リストに追加 (Add to List)] をクリックします。これにより、サービスが「サービス」ドロップダウンリストに追加されます。

Service Name :

Protocol :

Port Range : to

Service List:

- 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]
- Service1[UDP/5060~5070]**

注：サービスリストからサービスを削除する場合は、サービスリストからサービスを選択して、Deleteをクリックします。サービスエントリを更新する場合は、サービスリストから更新するサービスを選択し、Updateをクリックします。リストに別の新しいサービスを追加するには、Add Newをクリックします。

ステップ 11[OK] をクリックします。これにより、ウィンドウが閉じ、ユーザがアクセスルールページに戻ります。

注：Add Newをクリックする場合は、ステップ7～11に従ってください。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length: /

Destination IP / Prefix Length: /

ステップ 12アクセスルールに一致するパケットをログに記録するには、LogドロップダウンリストでLog packets match this ruleを選択します。それ以外の場合は、Not Logを選択します。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

 ✓

 ✓

Source IP / Prefix Length: /

Destination IP / Prefix Length: /

ステップ 13Source Interfaceドロップダウンリストから、このルールの影響を受けるインターフェイスを選択します。送信元インターフェイスは、トラフィックが開始されるインターフェイスです。

- ・ LAN : ルータのローカルエリアネットワーク。
- ・ WAN1 : ワイドエリアネットワーク、またはルータがISPやネクストホップルータからインターネットを取得するネットワーク。
- ・ WAN2 : セカンダリネットワークである点を除き、WAN1と同じです。
- ・ ANY : 任意のインターフェイスの使用を許可します。

The screenshot shows the 'Access Rules' configuration interface. The 'Source IP / Prefix Length' dropdown menu is open, with 'Single' selected and highlighted in blue. The 'Destination IP / Prefix Length' field is set to '/ 128'. The 'Action' is set to 'Allow', 'Service' is 'All Traffic [TCP&UDP/1~65535]', and 'Log' is 'Log packets match this rule'. The 'Source Interface' is 'LAN'. There are 'Save' and 'Cancel' buttons at the bottom.

ステップ 14 : Source IP ドロップダウンリストで、アクセスルールが適用される送信元 IP アドレスを指定するオプションを選択します。

- ・ Any : 送信元インターフェイスからのすべてのトラフィックにアクセスルールが適用されます。ドロップダウンリストの右側に使用可能なフィールドはありません。
- ・ Single : アクセスルールは、送信元インターフェイスからの単一の IP アドレスに適用されます。アドレスフィールドに目的の IP アドレスを入力します。
- ・ サブネット : アクセスルールは、送信元インターフェイスからサブネットネットワークに適用されます。IP アドレスとプレフィクス長を入力します。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP / Prefix Length:

Destination IP / Prefix Length: /

ステップ 15 : Destination IPドロップダウンリストで、アクセスルールが適用される宛先IPアドレスを指定するオプションを選択します。

- ・ Any : 宛先インターフェイスへのすべてのトラフィックにアクセスルールが適用されます。ドロップダウンリストの右側に使用可能なフィールドはありません。
- ・ Single : アクセスルールは、単一のIPアドレスに対して宛先インターフェイスに適用されます。アドレスフィールドに目的のIPアドレスを入力します。
- ・ サブネット : アクセスルールがサブネットネットワーク上で宛先インターフェイスに適用されます。IPアドレスとプレフィクス長を入力します。

ステップ 16 : Saveをクリックして、IPv6アクセスルールに対するすべての変更を保存します。

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。