

# RV0xxでIPv6のサービストラフィックを許可またはブロックする

## 目的

このドキュメントでは、要求が特定のマシンから発信された場合に、特定のスケジュールに基づいてサービストラフィックを許可またはブロックする方法について説明します。この記事では、IPアドレスに基づいてユーザを拒否できると説明しています。スケジュールは任意の日または時間に基づいて作成できます。許可または拒否されるIPアドレスは、特定の範囲または特定のIPアドレスにすることができます。

## 適用可能なデバイス

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

## サービストラフィックを許可またはブロックする手順

### サービスの設定手順

ステップ 1 : Router Configuration Utility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 1-5 of 7 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"/>	Allow	All Traffic [1]	WAN1	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN2	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Add Restore to Default Rules

Page 1 of 2

ステップ 2 : Addをクリックして、サービストラフィックスケジュールを作成します。アクセスルールページが開きます。

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 3 : Actionドロップダウンリストで、Allowを選択してトラフィックが通過できるようにするか、Denyを選択してトラフィックをブロックします。

## Access Rules

**Services**

Action :

Service :  

Log :

Source Interface :

Source IP :

Destination IP :

**Scheduling**

Time :

From :   (hh:mm)

Effective on :  Every  Mon  Tue  Wed  Thu  Fri  Sat

- 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]

ステップ 4 : Service ドロップダウンリストからサービスを選択します。

注 : Service ドロップダウンリストに特定のサービスが表示されていない場合は、Service Management をクリックします。

## 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 : 「ログ」ド롭ダウンリストからオプションを選択します。

- ・ ログパケットがこのルールに一致 – アクセスルールに一致する着信パケットをログに記録します。
- ・ Not Log : アクセスルールに一致する着信パケットをログに記録しません。

## 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

手順 6 : Source Interface ドロップダウンリストから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 : ローカルエリアネットワーク。オフィスビルや学校などのネットワーク上でコンピュータを近くで接続する。
- ・ WAN1 : ワイドエリアネットワーク。これは、ネットワーク上の広いエリアのコンピュータを接続します。これは、地域または国を接続する任意のネットワークである可能性があります。企業や政府が他の場所に接続するために使用されます。
- ・ WAN2:2番目のネットワークである点を除き、WAN1と同じです。
- ・ DMZ:LANを公開せずに、外部トラフィックがネットワーク上のコンピュータにアクセスできるようにします。

- ・ ANY : 任意のインターフェイスの使用を許可します。

### 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

手順 7 : Source IP ドロップダウンリストから、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 : トラフィックの転送に任意の IP アドレスが使用されます。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 : 単一の IP アドレスを使用してトラフィックを転送します。ドロップダウンリストの右側のフィールドに目的の IP アドレスを入力します。
- ・ Range : トラフィックの転送に範囲 IP アドレスが使用されます。ドロップダウンリストの右側のフィールドに、目的の IP アドレス範囲を入力します。

## 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 8 : Destination IP ドロップダウンリストから、宛先 IP アドレスを指定するオプションを選択します。

- ・ Any : トラフィックの転送に任意の IP アドレスが使用されます。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 : 単一の IP アドレスを使用してトラフィックを転送します。ドロップダウンリストの右側のフィールドに目的の IP アドレスを入力します。
- ・ Range : トラフィックの転送に範囲 IP アドレスが使用されます。ドロップダウンリストの右側のフィールドに、目的の IP アドレス範囲を入力します。

スケジューリングの設定手順

## 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 1 : 「時間」 ドロップダウンリストから時間オプションを選択します。

- ・ Always : このオプションは、1週間を通してサービストラフィックを許可またはブロックします。
- ・ 間隔 : このオプションは、特定の日または特定の時刻の日にサービストラフィックを許可またはブロックします。

## 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 2 : FromフィールドとToフィールドに特定の時刻を入力して、サービストラフィックを許可またはブロックする時刻を指定します。

## 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 3 : デフォルトで[毎日]チェックボックスをオンのままにして毎日サービストラフィックを特定の時刻に許可またはブロックするか、[毎日]チェックボックスをオフにしてサービストラフィックを許可またはブロックする日を選択します。

ステップ 4 : Saveをクリックして、設定したアクセスルールを保存します。

## 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。