

# RV016、RV042、RV042G、およびRV082 VPNルータの特定のサイトでのHTTPSアクセス のブロック

## 目的

Hyper Text Transfer Protocol Secure(HTTPS)は、Hyper Text Transfer Protocol(HTTP)とSSL/TLSプロトコルを組み合わせ、暗号化された通信または安全な通信を提供します。

このドキュメントでは、ユーザが目的のhttps WebサイトまたはURLにアクセスするのをブロックする方法について説明します。これは、セキュリティやペアレナタルコントロールなどの他の理由で、不要なサイトや既知の悪意のあるサイトをブロックするのに役立ちます。

## 適用可能なデバイス

- RV016
- RV042
- RV042G
- RV082

## [Software Version]

- 4.2.2.08

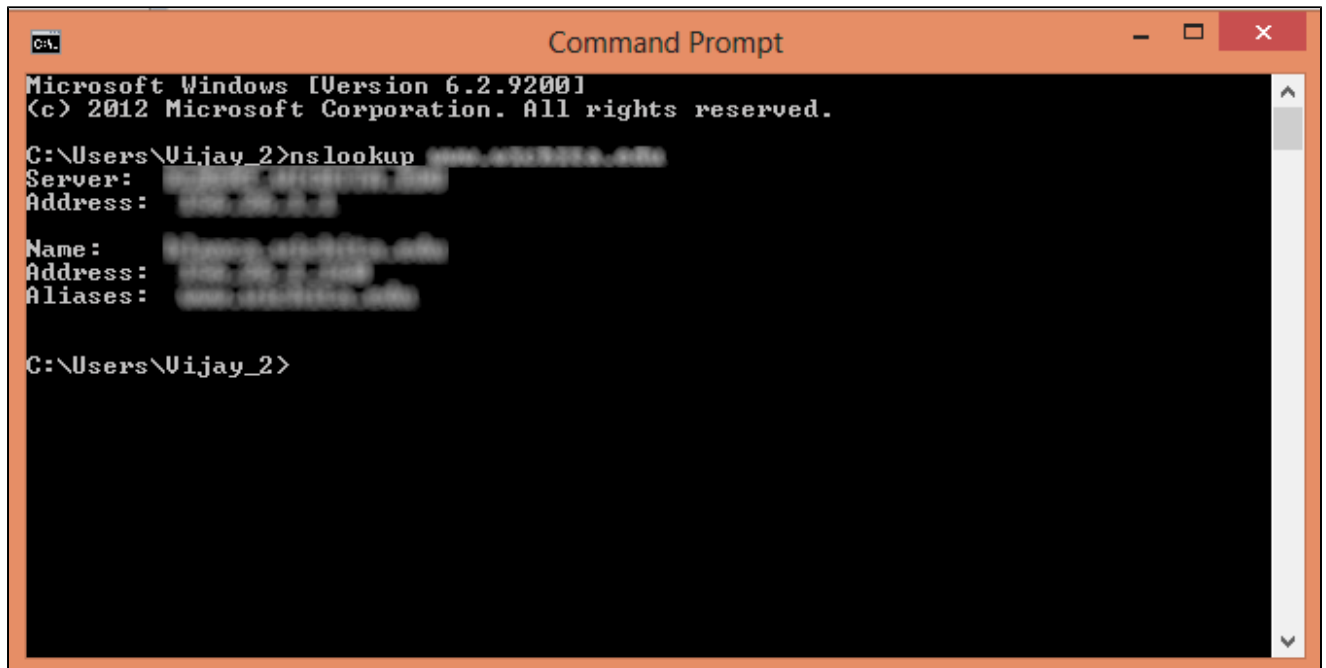
## HTTPSアクセスのブロック

ブロックする特定のWebサイトのIPアドレスを見つける必要があります。これを行うには、次のステップ1および2に従ってください。

ステップ 1 : PCで、Start > Runの順に選択してコマンドプロンプトを開きます。次に、Openフィールドにcmdと入力します。(Windows 8では、スタート画面にcmdと入力するだけです)。

ステップ 2 : コマンドプロンプトウィンドウで、nslookup <space> URLと入力します。

URLは、ブロックするWebサイトです。たとえば、Webサイト「www.example.com」をブロックするには、次のように入力します。  
nslookup www.example.comです。



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Vijay_2>nslookup www.example.com
Server:          192.168.1.1
Address:         192.168.1.1

Name:           www.example.com
Address:        93.184.216.34
Aliases:        www.example.com

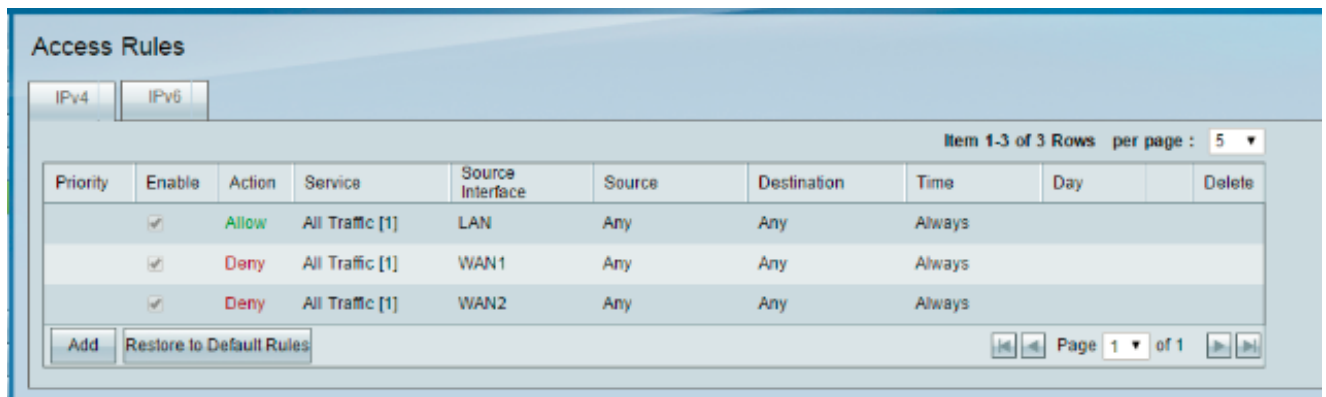
C:\Users\Vijay_2>
```

次のフィールドが表示されます。

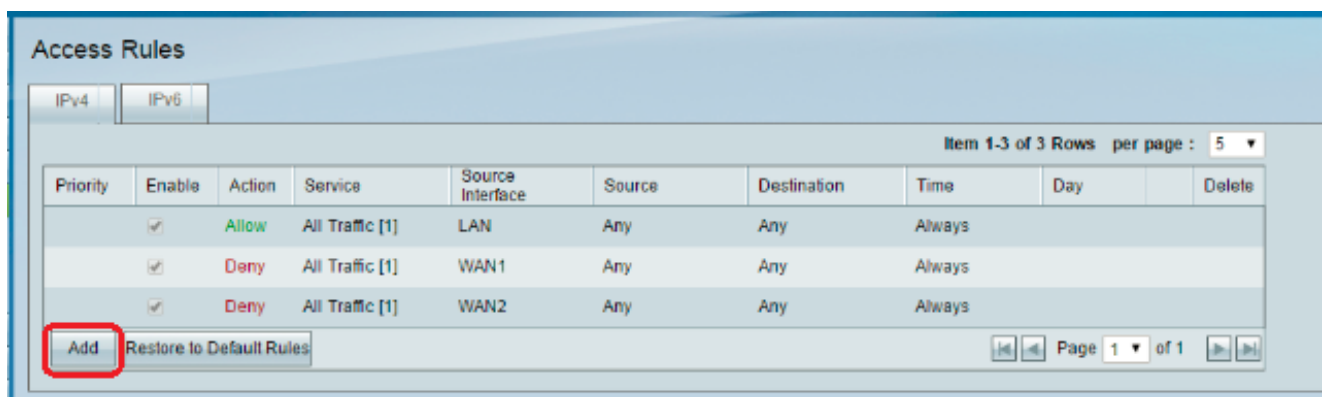
- Server : ルータに情報を提供するDNSサーバの名前を表示します。
- Address : ルータに情報を提供するDNSサーバのIPアドレスを表示します。
- Name : ステップ2で入力したWebサイトをホストするサーバの名前が表示されます。
- Address : ステップ2で入力したWebサイトをホストするサーバのIPアドレスが表示されます。
- Aliases : 手順2で入力したWebサイトをホストするサーバの完全修飾ドメイン名 (FQDN)が表示されます。

Webサイトのサーバアドレスは必要です。

ステップ 3 : Router Configuration Utilityにログインして、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。



ステップ 4 : Addをクリックして、新しいルールを追加します。Access Rulesウィンドウが表示されます。



ステップ 5 : ActionドロップダウンリストからDenyを選択し、目的のWebサイトをブロックします。

## Access Rules

Services

Action : **Deny** ▼

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

Log : Log packets match this rule ▼

Source Interface : LAN ▼

Source IP : Single ▼

Destination IP : Single ▼

---

### Scheduling

Time : Always ▼

From : 00:00 (hh:mm) To : 00:00 (hh:mm)

Effective on :  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

手順 6 : HTTPS URLをブロックするため、ServiceドロップダウンリストからHTTPS [TCP/443~443] を選択します。

## 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 : Log ドロップダウンリストから、Log Management に必要なオプションを選択します。

## 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

- ・ ログパケットがこのルールに一致する：ブロックされたパケットをログに記録します。
- ・ Not log：パケットをログに記録しません。

ステップ 8：ルータのLANインターフェイスからのURL要求をブロックする必要があるため、Source Interface ドロップダウンリストからLANを選択します。

## 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 9 : Source IP ドロップダウンリストから目的のオプションを選択します。次に、Web サイトへのアクセスが許可されていないマシンの IP アドレスを入力します。

## 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

- ・ Single : このルールは、LANインターフェイスの単一のIPアドレスからのパケットをブロックします。
- ・ Range : このルールは、LANインターフェイスでIPアドレスの範囲 ( IPv4のみ ) からのパケットをブロックします。範囲の最初のIPアドレスを最初のフィールドに入力し、最後のIPアドレスを2番目のフィールドに入力します。
- ・ ANY : このルールはLANインターフェイスのすべてのIPアドレスに適用されます。

ステップ 10 : Destination IP ドロップダウンリストから目的のオプションを選択します。次に、ブロックするURLのIPアドレスを入力します。この情報を見つけるには、ステップ1とステップ2を参照してください。



## 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

・ Single : このルールは、LANインターフェイスの単一のIPアドレスからのパケットをブロックします。

・ Range : このルールは、LANインターフェイスでIPアドレスの範囲 ( IPv4のみ ) からのパケットをブロックします。範囲の最初のIPアドレスを最初のフィールドに入力し、最後のIPアドレスを2番目のフィールドに入力します。通常、このオプションは不正確になることがあり、他のWebサイトをブロックするため、使用されません。

ステップ 11 Schedulingセクションで目的のスケジューリング・オプションを選択します。

## 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

- ・ 常時 : このルールは常にWebサイトをブロックします。
- ・ 間隔 : このルールは、特定の時間または曜日にのみWebサイトをブロックします。

ステップ 12手順11でIntervalを選択した場合は、目的の開始時刻と終了時刻をFromフィールドとToフィールドに入力します。

## 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 13ステップ11でIntervalを選択した場合は、Webサイトをブロックする対象の日をチェックするか、またはEverydayチェックボックスをオンにして、毎日そのWebサイトをブロックします。

## Access Rules

### Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

### Scheduling

Time :

From :  (hh:mm) To :  (hh:mm)

Effective on :  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

ステップ 14 : [Save] をクリックして、設定を保存します。指定したWebサイトはブロックされます。

## 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

さらにURLをブロックするには、[ステップ1](#) ~ 15を繰り返します。

## 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。