

在RV016、RV042、RV042G和RV082 VPN路由器上阻止特定站點的HTTPS訪問

目標

超文本傳輸協定安全(HTTPS)是超文本傳輸協定(HTTP)與SSL/TLS協定的組合，以提供加密通訊或安全通訊。

本文說明如何阻止使用者訪問所需的https網站或URL。這將幫助使用者出於安全原因和其他原因（如家長控制）阻止不需要的或已知的惡意站點。

適用裝置

- RV016
- RV042
- RV042G
- RV082

軟體版本

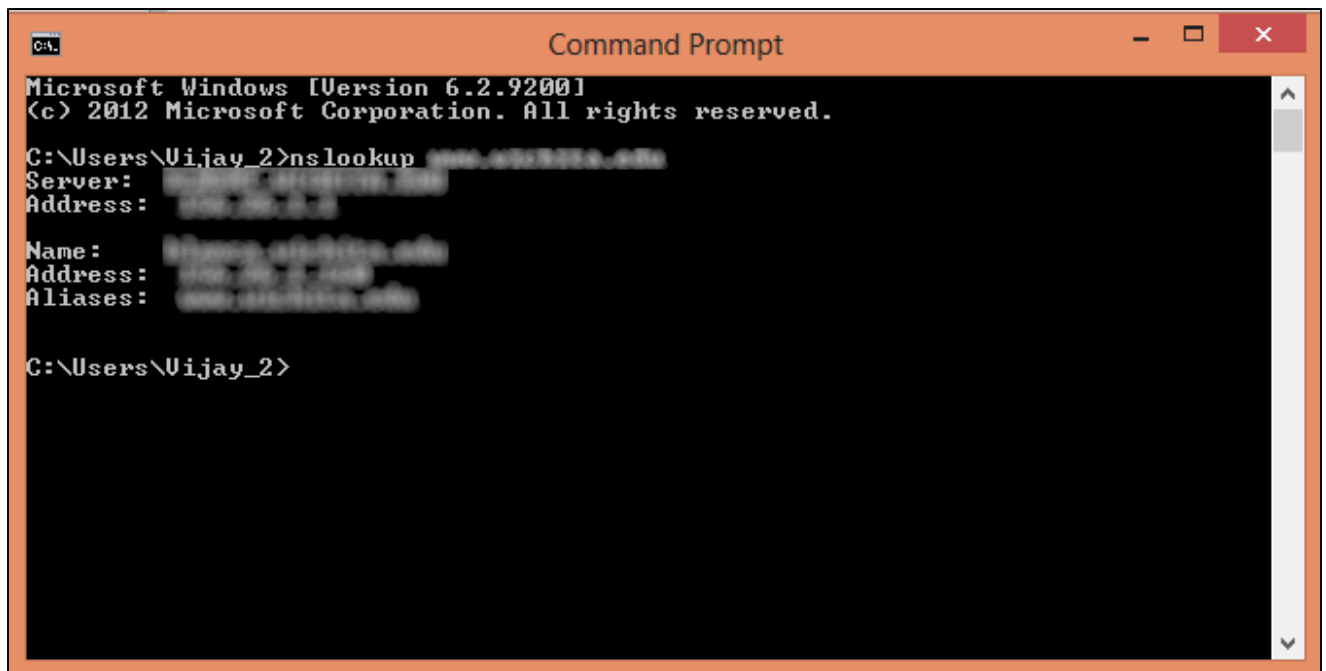
- 4.2.2.08

阻止HTTPS訪問

您需要找到要阻止的特定網站的IP地址。為此，請遵循以下步驟1和2。

步驟 1.在PC上，通過Start > Run開啟命令提示符。然後在開啟欄位中鍵入cmd。（在Windows 8中，只需在開始螢幕中鍵入cmd。）

步驟 2.在「命令提示符」視窗中，輸入nslookup <space> URL。URL是要阻止的網站。例如，如果要阻止網站「www.example.com」，您應該輸入：
nslookup www.example.com。



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

C:\Users\Vijay_2>nslookup www.vijay2.com
Server:          192.168.1.1
Address:         192.168.1.1

Name:           www.vijay2.com
Address:        192.168.1.100
Aliases:        www.vijay2.com

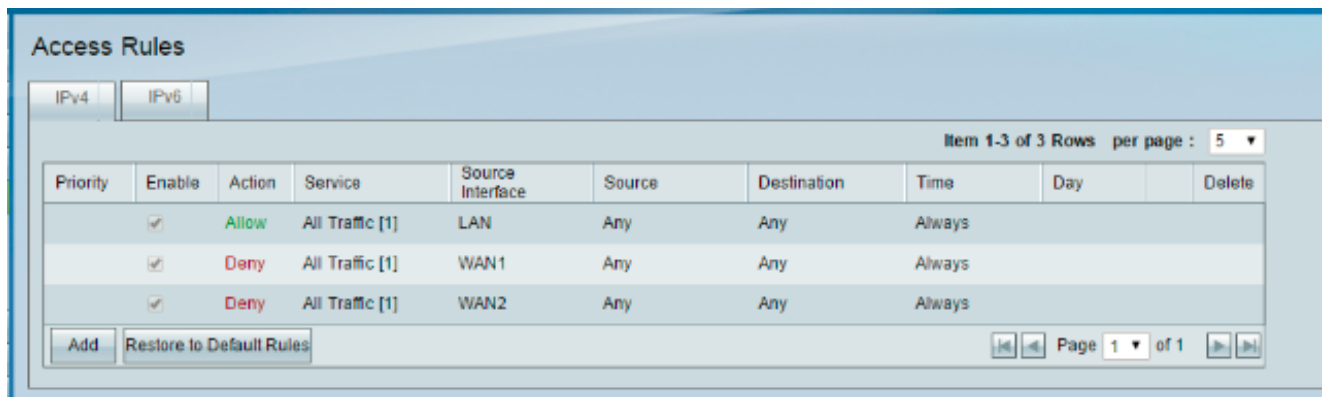
C:\Users\Vijay_2>
```

將顯示以下欄位：

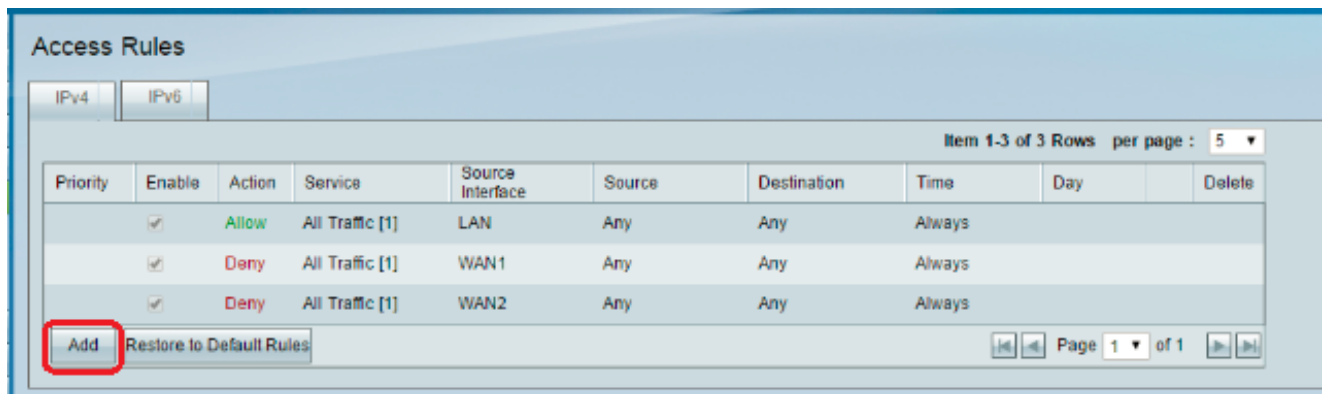
- 伺服器 — 顯示向路由器提供資訊的DNS伺服器的名稱。
- 地址 — 顯示向路由器提供資訊的DNS伺服器的IP地址。
- 名稱 — 顯示託管您在步驟2中輸入的網站的伺服器的名稱。
- 地址 — 顯示託管您在步驟2中輸入的網站的伺服器的IP地址。
- 別名 — 顯示託管您在步驟2中輸入的網站的伺服器的完全限定域名(FQDN)。

網站的伺服器地址就是我們需要的。

步驟 3.登入到路由器配置實用程式以選擇Firewall > Access Rules。Access Rule頁面隨即開啟：



步驟 4. 按一下Add新增新規則。此時會顯示Access規則視窗：



步驟 5. 從Action下拉選單中選擇Deny以阻止所需的網站。

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

步驟 6. 由於我們正在封鎖HTTPS URL，請從「服務」下拉選單中選擇HTTPS [TCP/443~443]。

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

步驟 7. 從Log下拉選單中選擇所需的日誌管理選項。

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

·記錄與此規則匹配的資料包 — 將記錄被阻止的資料包。

·不記錄 — 不記錄任何資料包。

步驟 8.從Source Interface下拉選單中選擇LAN，因為我們必須阻止將來自路由器LAN介面的URL請求。

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

步驟 9. 從Source IP下拉選單中選擇所需的選項。然後輸入不允許訪問該網站的電腦的IP地址：

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 — 規則阻止來自LAN介面中單個IP地址的資料包。

·範圍 — 規則會攔截來自LAN介面中一系列IP地址（僅限IPv4）的資料包。在第一個欄位中輸入範圍的第一個IP地址，然後在第二個欄位中輸入最終IP地址。

· ANY — 規則適用於LAN介面中的所有IP地址。

步驟 10.從Destination IP下拉清單中選擇所需的選項。然後輸入要阻止的URL的IP地址。請參閱步驟1和步驟2以幫助您找到此資訊。

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 — 規則阻止來自LAN介面中單個IP地址的資料包。

· 範圍 — 規則會攔截來自LAN介面中一系列IP地址（僅限IPv4）的資料包。在第一個欄位中輸入範圍的第一個IP地址，然後在第二個欄位中輸入最終IP地址。通常，不會使用此選項，因為它有時會不準確，並且會阻止其他網站。

步驟 11. 在「計畫」部分中選擇所需的計畫選項。

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

·始終 — 此規則始終阻止網站。

·間隔 — 此規則僅在一週中的特定時間或日期阻止網站。

步驟 12. 如果在第11步選擇Interval，請在From和To欄位中輸入所需的開始和結束時間。

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

步驟 13. 如果您在 Step 11 選擇 Interval，請選中想要阻止網站的日期，或選中 Everyday 覈取方塊以每天阻止網站。

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

步驟 14. 按一下「Save」以儲存設定。將阻止指定的網站。

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

重做[步驟1](#)到步驟15以阻止更多URL。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。