

RV016, RV042, RV042G 및 RV082 VPN Router에서 특정 사이트에 대한 HTTPS 액세스 차단

목표

HTTPS(Hyper Text Transfer Protocol Secure)는 암호화된 통신 또는 보안 통신을 제공하기 위해 HTTP(Hyper Text Transfer Protocol)와 SSL/TLS 프로토콜의 조합입니다.

이 문서에서는 사용자가 원하는 https 웹 사이트 또는 URL에 액세스하지 못하도록 차단하는 방법에 대해 설명합니다. 이는 사용자가 보안 및 자녀 보호 등의 기타 이유로 원치 않거나 알려진 악성 사이트를 차단하는 데 도움이 됩니다.

적용 가능한 디바이스

- RV016
- RV042
- RV042G
- RV082

소프트웨어 버전

- 4.2.2.08

HTTPS 액세스 차단

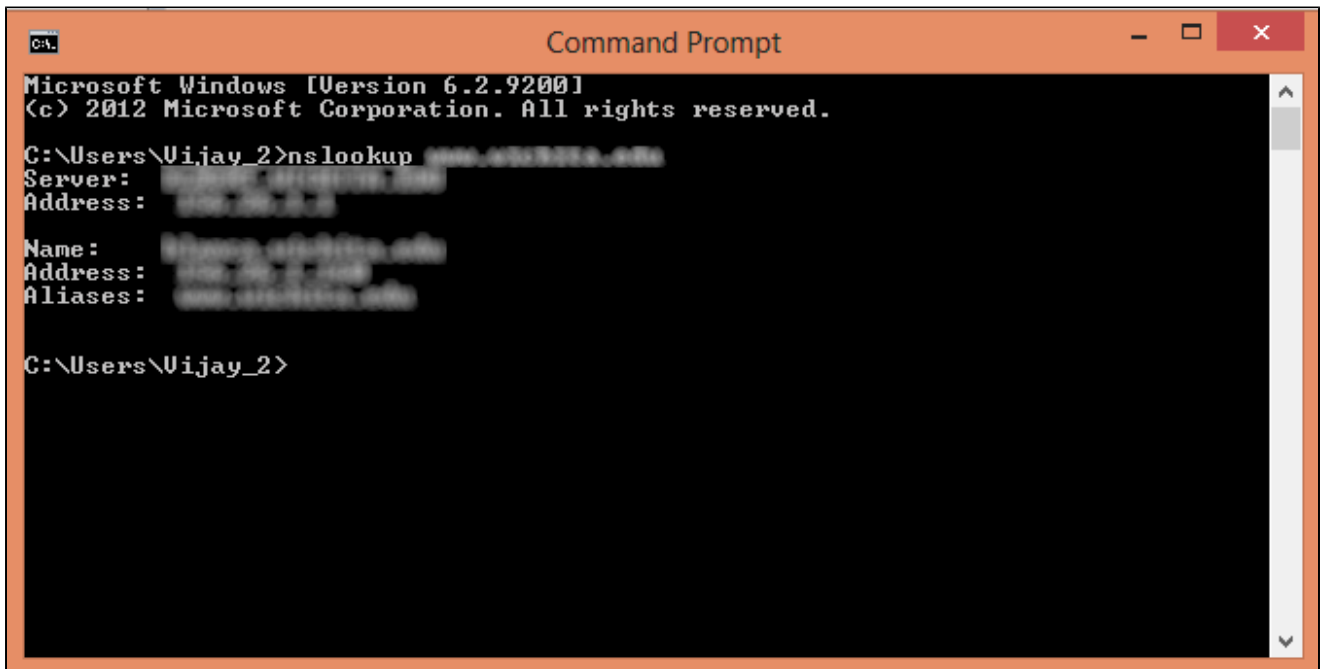
차단하려는 특정 웹 사이트의 IP 주소를 찾아야 합니다. 이를 위해서는 아래의 1단계와 2단계를 따르십시오.

1단계. PC에서 Start(시작) > Run(실행)을 선택하여 명령 프롬프트를 엽니다. 그런 다음 열기 필드에 cmd를 입력합니다. (Windows 8의 경우 시작 화면에 cmd를 입력합니다.)

2단계. Command Prompt(명령 프롬프트) 창에 nslookup <space> URL을 입력합니다. URL은 차단하려는 웹 사이트입니다. 예를 들어, 웹 사이트 "www.example.com"를 차단하려면 다음

을 입력합니다.

nslookup www.example.com.



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

C:\Users\Vijay_2>nslookup www.example.com
Server:          [redacted]
Address:         [redacted]

Name:           [redacted]
Address:        [redacted]
Aliases:        [redacted]

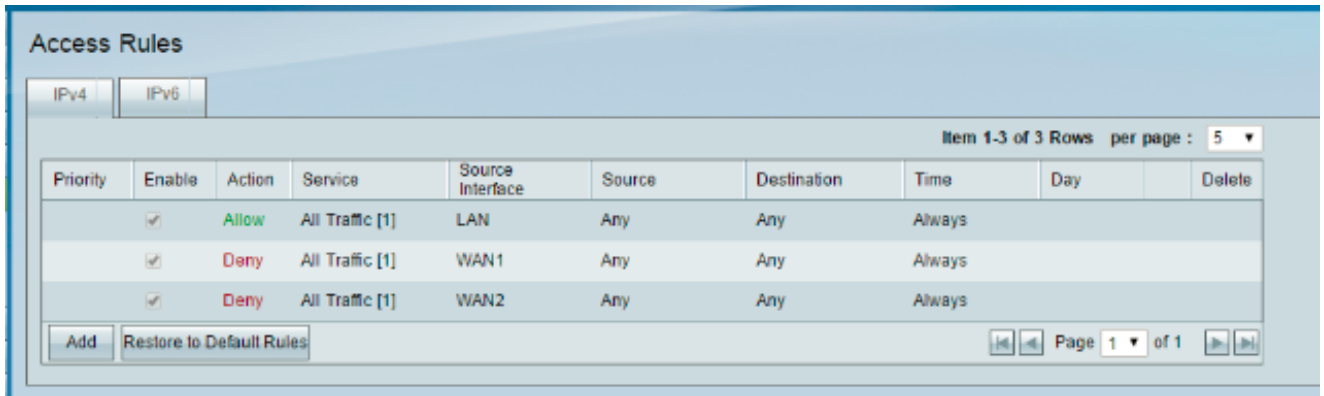
C:\Users\Vijay_2>
```

다음 필드가 표시됩니다.

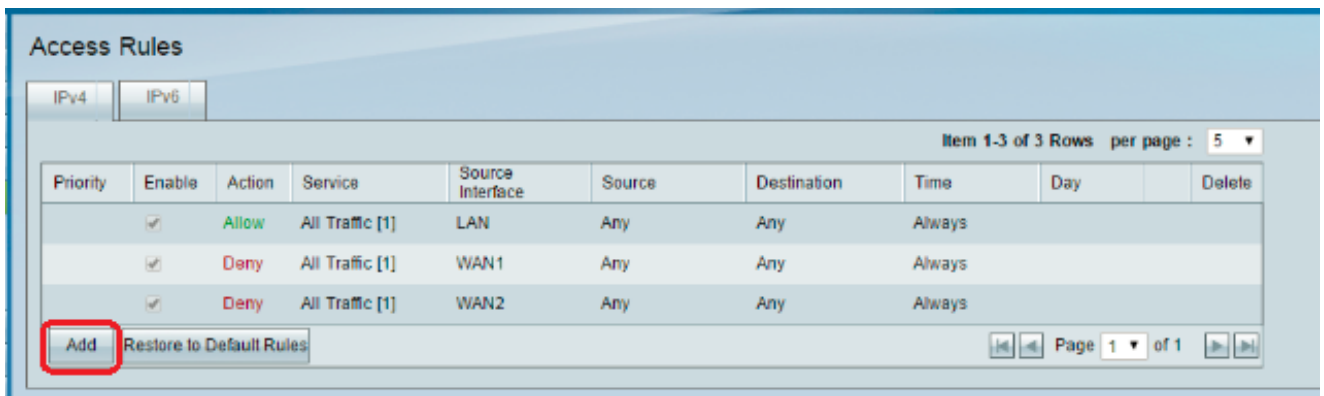
- 서버 — 라우터에 정보를 제공하는 DNS 서버의 이름을 표시합니다.
- Address — 라우터에 정보를 제공하는 DNS 서버의 IP 주소를 표시합니다.
- 이름 — 2단계에서 입력한 웹 사이트를 호스팅하는 서버의 이름을 표시합니다.
- Address — 2단계에서 입력한 웹 사이트를 호스팅하는 서버의 IP 주소를 표시합니다.
- 별칭 — 2단계에서 입력한 웹 사이트를 호스팅하는 서버의 FQDN(Fully Qualified Domain Name)을 표시합니다.

웹사이트의 서버 주소가 우리에게 필요한 것입니다.

3단계. Router Configuration Utility에 로그인하여 Firewall(방화벽) > Access Rules(액세스 규칙)를 선택합니다. Access Rule 페이지가 열립니다.



4단계. 새 규칙을 추가하려면 Add를 클릭합니다. Access Rules 창이 나타납니다.



5단계. 원하는 웹 사이트를 차단하려면 Action(작업) 드롭다운 목록에서 Deny(거부)를 선택합니다.

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

6단계. HTTPS URL을 차단하고 있으므로 서비스 드롭다운 목록에서 HTTPS [TCP/443~443]을 선택합니다.

Access Rules

Services

Action : Deny ▾

Service : **HTTPS [TCP/443~443]** ▾
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

7단계. Log 드롭다운 목록에서 Log Management에 대해 원하는 옵션을 선택합니다.

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

· Log packets match this rule — 차단된 패킷을 기록합니다.

· Not log — 패킷을 기록하지 않습니다.

8단계. 라우터 LAN 인터페이스에서 오는 URL 요청을 차단해야 하므로 Source Interface 드롭 다운 목록에서 LAN을 선택합니다.

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

9단계. Source IP(소스 IP) 드롭다운 목록에서 원하는 옵션을 선택합니다. 그런 다음 웹 사이트에 액세스할 수 없는 컴퓨터의 IP 주소를 입력합니다.

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 — 규칙은 LAN 인터페이스의 단일 IP 주소에서 패킷을 차단합니다.

· Range — 규칙은 LAN 인터페이스의 IP 주소 범위(IPv4만 해당)에서 패킷을 차단합니다. 첫 번째 필드에 범위의 첫 번째 IP 주소를 입력한 다음 두 번째 필드에 최종 IP 주소를 입력합니다.

· ANY — 규칙이 LAN 인터페이스의 모든 IP 주소에 적용됩니다.

10단계. Destination IP 드롭다운 목록에서 원하는 옵션을 선택합니다. 그런 다음 차단할 URL의 IP 주소를 입력합니다. 이 정보를 찾으려면 1단계와 2단계를 참조하십시오.

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 — 규칙은 LAN 인터페이스의 단일 IP 주소에서 패킷을 차단합니다.

· Range — 규칙은 LAN 인터페이스의 IP 주소 범위(IPv4만 해당)에서 패킷을 차단합니다. 첫 번째 필드에 범위의 첫 번째 IP 주소를 입력한 다음 두 번째 필드에 최종 IP 주소를 입력합니다 . 이 옵션은 일반적으로 사용되지 않습니다. 때로는 부정확할 수 있으며 다른 웹 사이트를 차단합니다.

11단계. Scheduling(예약) 섹션에서 원하는 예약 옵션을 선택합니다.

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

· Always — 이 규칙은 항상 웹 사이트를 차단합니다.

· Interval — 이 규칙은 특정 시간 또는 요일에 대해서만 웹 사이트를 차단합니다.

12단계. 단계 11에서 간격을 선택한 경우 시작 및 종료 필드에 원하는 시작 및 종료 시간을 입력합니다.

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

13단계. 11단계에서 Interval(간격)을 선택한 경우, 원하는 요일에 웹 사이트를 차단하거나 Everyday(매일) 확인란을 선택하여 매일 웹 사이트를 차단합니다.

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

14단계. Save(저장)를 클릭하여 설정을 저장합니다. 지정한 웹 사이트가 차단됩니다.

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

추가 URL을 차단하려면 1단계에서 15단계로 다시 실행합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.