

Bloquear o acesso HTTPS para um site específico nos roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

O protocolo HTTPS é uma combinação do protocolo HTTP com protocolo SSL/TLS para fornecer comunicação criptografada ou comunicação segura.

Este documento explica como impedir que os usuários acessem os sites ou URLs https desejados. Isso ajudará o usuário a bloquear sites mal-intencionados indesejados ou conhecidos por motivos de segurança e outros, como controles dos pais.

Dispositivos aplicáveis

- RV016
- RV042
- RV042G
- RV082

Versão de software

- 4.2.2.08

Bloquear acesso HTTPS

Você precisa encontrar o endereço IP do site específico que deseja bloquear. Para fazer isso, siga as etapas 1 e 2 abaixo.

[Etapa 1.](#) No PC, abra o prompt de comando **Start > Run**. Em seguida, digite **cmd** no campo Abrir. (No Windows 8, digite **cmd** na **tela Iniciar**.)

Etapa 2. Na janela Command Prompt, digite **nslookup <space> URL**. O URL é o site que você deseja bloquear. Por exemplo, se você quiser bloquear o site "www.example.com", digite:
nslookup www.example.com.

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

C:\Users\Uijay_2>nslookup www.ataidirect.com
Server:
Address: 192.168.1.1

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

C:\Users\Uijay_2>
```

Os seguintes campos serão exibidos:

Servidor — Exibe o nome do servidor DNS que fornece informações ao roteador.

Endereço — Exibe o endereço IP do servidor DNS que fornece informações ao roteador.

Nome — Exibe o nome do servidor que hospeda o site inserido na Etapa 2.

Endereço — Exibe o endereço IP do servidor que hospeda o site inserido na Etapa 2.

Aliases — Exibe o Nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o site que você inseriu na Etapa 2.

O endereço do servidor do site é o que precisamos.

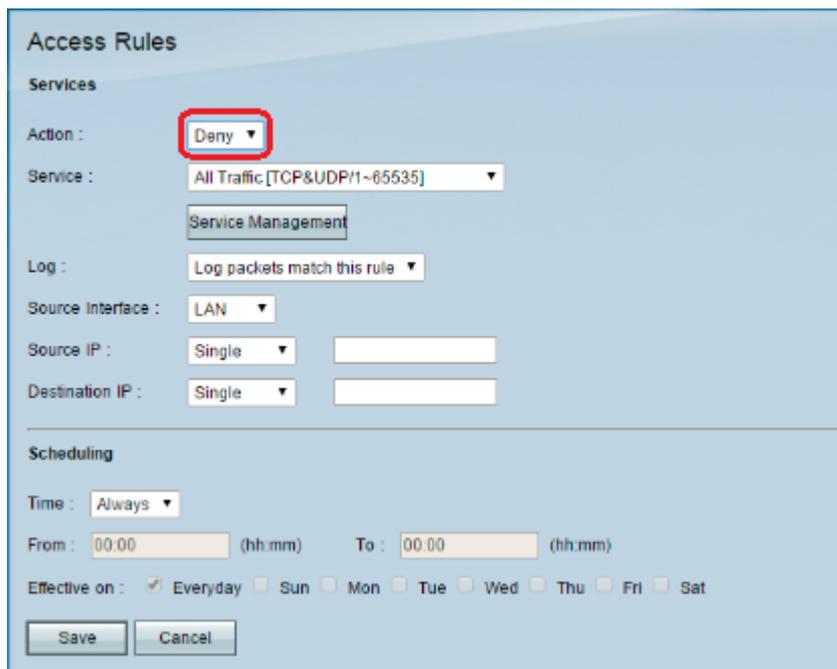
Etapa 3. Efetue login no Utilitário de configuração do roteador para escolher **Firewall > Regras de acesso**. A página *Regra de Acesso* é aberta:

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		

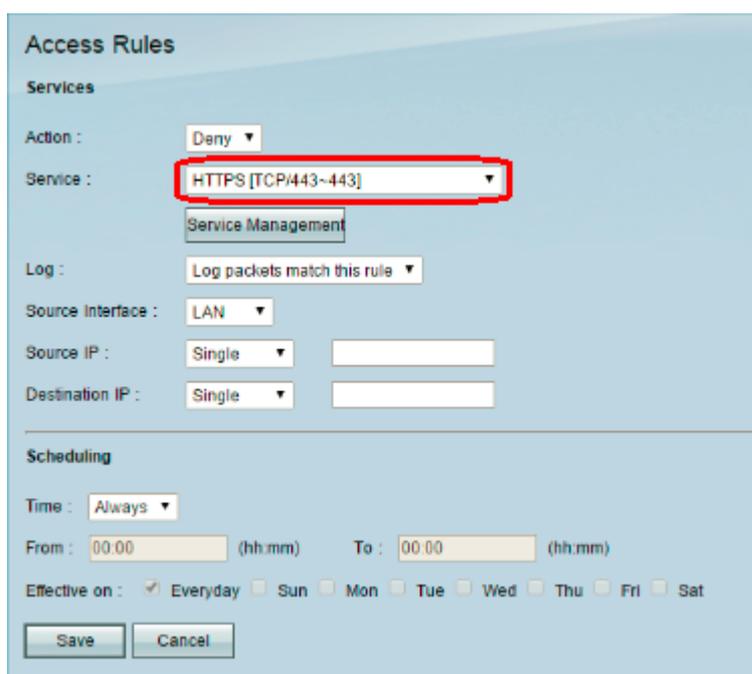
Etapa 4. Clique em **Adicionar** para adicionar uma nova regra. A janela *Regras de acesso* é exibida:



Etapa 5. Escolha **Negar** na lista suspensa Ação para bloquear o site desejado.



Etapa 6. Escolha **HTTPS [TCP/443~443]** na lista suspensa Serviço enquanto estamos bloqueando um URL HTTPS.



Passo 7. Escolha a opção desejada para Gerenciamento de log na lista suspensa Log.

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

Save Cancel

Os pacotes de log correspondem a essa regra — Registrarão os pacotes que estão bloqueados.

Não registrar — Não registrará nenhum pacote.

Etapa 8. Escolha **LAN** na lista suspensa Interface de origem, pois temos que bloquear a solicitação de URL que virá da interface LAN do roteador.

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

Save Cancel

Etapa 9. Escolha a opção desejada na lista suspensa IP de origem. Em seguida, insira o(s) endereço(s) IP da(s) máquina(s) que não tem permissão para acessar o site:

Access Rules

Services

Action : Deny

Service : HTTPS [TCP/443-443]

Service Management

Log : Log packets match this rule

Source Interface : LAN

Source IP : Single 192.168.1.100

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

Save Cancel

Single — A regra bloqueia pacotes de um único endereço IP na interface da LAN.

Intervalo — A regra bloqueia pacotes de um intervalo de endereços IP (somente IPv4) na interface LAN. Insira o primeiro endereço IP do intervalo no primeiro campo e, em seguida, o endereço IP final no segundo campo.

ANY — A regra se aplica a todos os endereços IP na interface LAN.

Etapa 10. Escolha a opção desejada na lista suspensa IP de destino. Em seguida, insira o endereço IP do URL que deseja bloquear. Consulte as Etapas 1 e 2 para ajudá-lo a encontrar essas informações.

Access Rules

Services

Action : Deny

Service : HTTPS [TCP/443-443]

Service Management

Log : Log packets match this rule

Source Interface : LAN

Source IP : Single 192.168.1.100

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

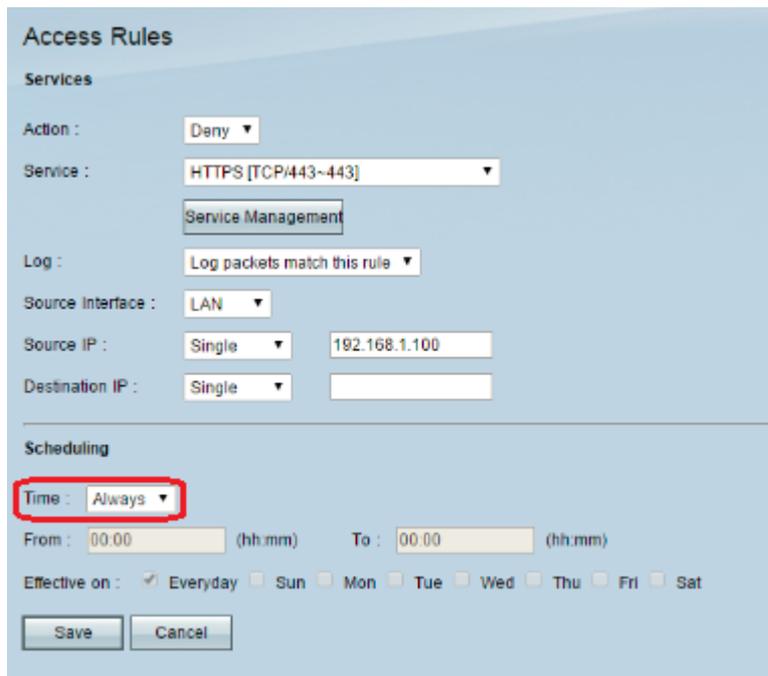
Save Cancel

Single — A regra bloqueia pacotes de um único endereço IP na interface da LAN.

Intervalo — A regra bloqueia pacotes de um intervalo de endereços IP (somente IPv4) na interface LAN. Insira o primeiro endereço IP do intervalo no primeiro campo e, em seguida,

o endereço IP final no segundo campo. Normalmente, essa opção não é usada, pois às vezes ela será imprecisa e bloqueará outros sites.

Etapa 11. Escolha a opção de agendamento desejada na seção Agendamento.

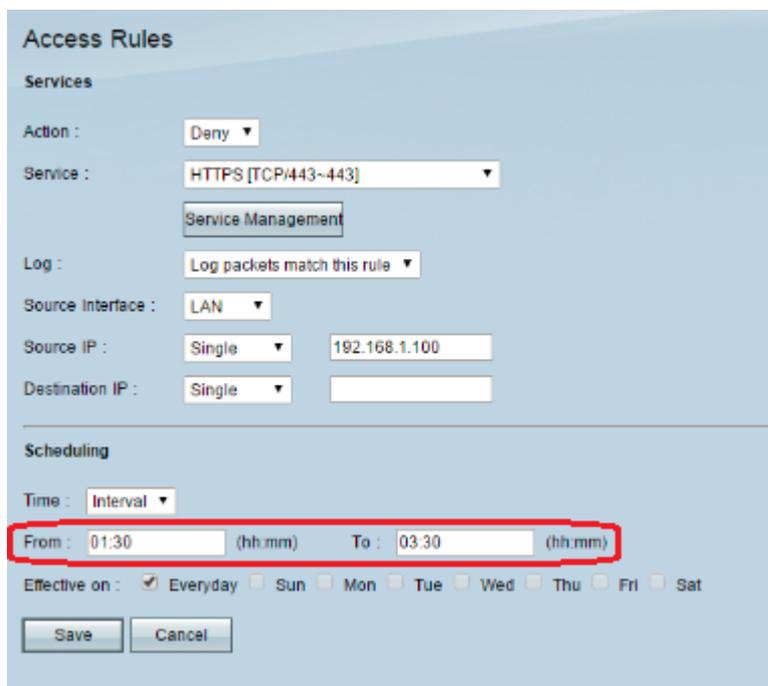


The screenshot shows the 'Access Rules' configuration interface. Under the 'Services' section, the 'Action' is set to 'Deny', the 'Service' is 'HTTPS [TCP/443-443]', and the 'Log' is 'Log packets match this rule'. The 'Source Interface' is 'LAN', the 'Source IP' is 'Single' with the value '192.168.1.100', and the 'Destination IP' is 'Single'. In the 'Scheduling' section, the 'Time' dropdown is highlighted with a red box and set to 'Always'. Below it, the 'From' and 'To' fields are both set to '00:00 (hh:mm)'. The 'Effective on' section has 'Everyday' checked and other days (Sun, Mon, Tue, Wed, Thu, Fri, Sat) unchecked. 'Save' and 'Cancel' buttons are at the bottom.

Sempre — Esta regra bloqueia o site o tempo todo.

Intervalo — Esta regra bloqueia o site somente em uma hora ou dia específicos da semana.

Etapa 12. Se você selecionar **Intervalo** na Etapa 11, insira as horas de início e término desejadas nos campos *De* e *Para*.



The screenshot shows the 'Access Rules' configuration interface, identical to the previous one, but with the 'Time' dropdown set to 'Interval'. The 'From' and 'To' fields in the 'Scheduling' section are highlighted with a red box and contain the values '01:30 (hh:mm)' and '03:30 (hh:mm)' respectively. The 'Effective on' section remains the same with 'Everyday' checked. 'Save' and 'Cancel' buttons are at the bottom.

Etapa 13. Se você selecionar **Intervalo** na Etapa 11, marque o(s) dia(s) desejado(s) no(s) qual(is) deseja bloquear o site ou marque a caixa de seleção **diária** para bloquear o site em cada dia.

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

Etapa 14. Clique em **Save** (Salvar) para salvar as configurações. O site especificado será bloqueado.

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

Refazer [Etapa 1](#) à Etapa 15 para bloquear mais URLs.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.