

Blocca accesso HTTPS per un sito specifico su RV016, RV042, RV042G e RV082 VPN Router

Obiettivo

Il protocollo HTTPS (Hyper Text Transfer Protocol Secure) è una combinazione di HTTP (Hyper Text Transfer Protocol) e SSL/TLS per fornire comunicazioni crittografate o sicure.

Questo documento spiega come impedire agli utenti di accedere ai siti Web o agli URL https desiderati. Ciò consente all'utente di bloccare siti dannosi noti o indesiderati per motivi di sicurezza e altri motivi, ad esempio il controllo genitori.

Dispositivi interessati

RV016
RV042
RV042G
RV082

Versione del software

•4.2.2.08

Blocca accesso HTTPS

È necessario trovare l'indirizzo IP del sito Web specifico che si desidera bloccare. A tale scopo, eseguire i passaggi 1 e 2 riportati di seguito.

[Passaggio 1](#). Sul PC, aprire il prompt dei comandi da **Start > Esegui**. Digitare quindi **cmd** nel campo Apri. In Windows 8, digitare **cmd** nella **schermata Start**.

Passaggio 2. Nella finestra del prompt dei comandi, immettere **nslookup <space> URL**. L'URL è il sito Web che si desidera bloccare. Ad esempio, se si vuole bloccare il sito "www.example.com" si deve inserire:
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.abc123.com
Server:          192.168.1.1
Address:         192.168.1.1
Name:           www.abc123.com
Address:        192.168.1.1
Aliases:        www.abc123.com

C:\Users\Uijay_2>
```

Verranno visualizzati i seguenti campi:

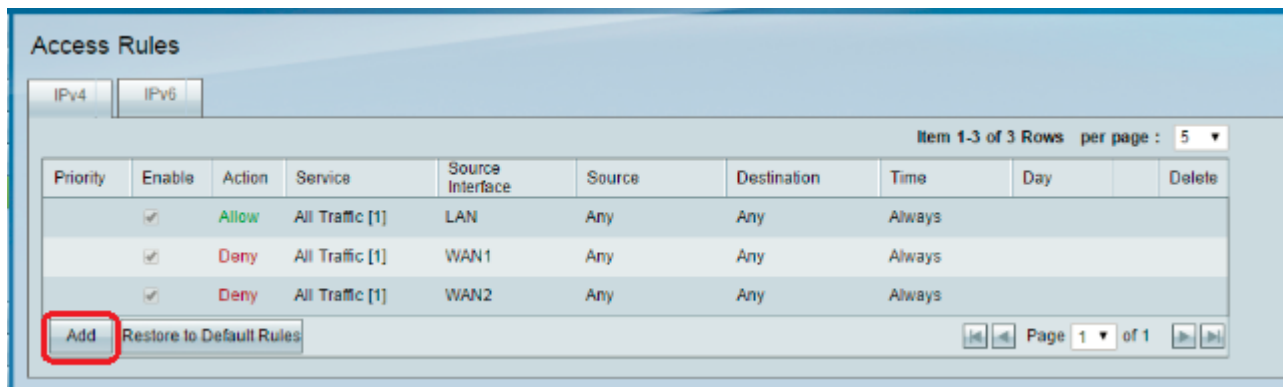
- Server: visualizza il nome del server DNS che fornisce informazioni al router.
- Indirizzo: visualizza l'indirizzo IP del server DNS che fornisce informazioni al router.
- Nome — visualizza il nome del server che ospita il sito Web immesso al punto 2.
- Indirizzo: visualizza l'indirizzo IP del server che ospita il sito Web immesso al punto 2.
- Alias: visualizza il nome di dominio completo (FQDN) del server che ospita il sito Web immesso al passo 2.

L'indirizzo del server del sito Web è quello di cui abbiamo bisogno.

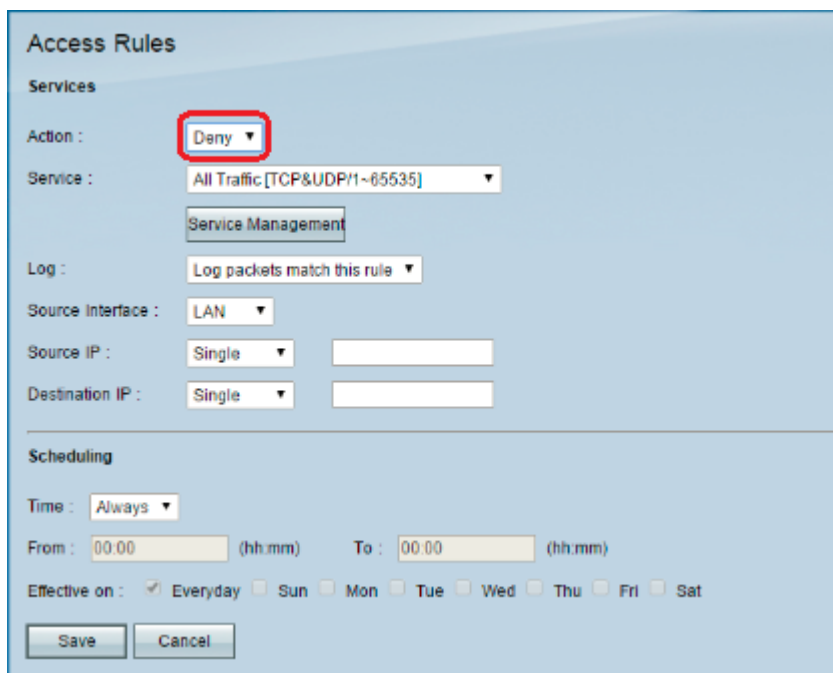
Passaggio 3. Accedere all'utility di configurazione del router per scegliere **Firewall > Regole di accesso**. Viene visualizzata la pagina *Regola di accesso*:

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		

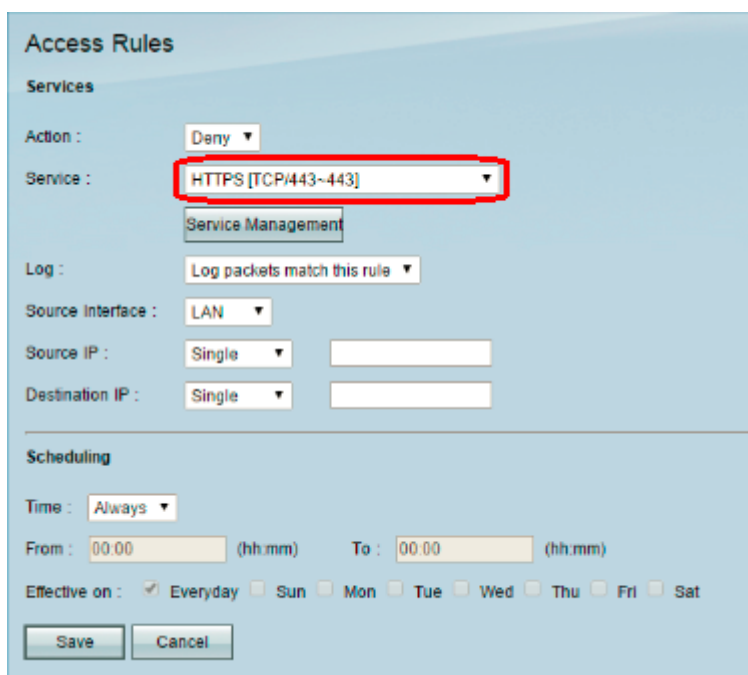
Passaggio 4. Fare clic su **Add** per aggiungere una nuova regola. Viene visualizzata la finestra *Access Rules*:



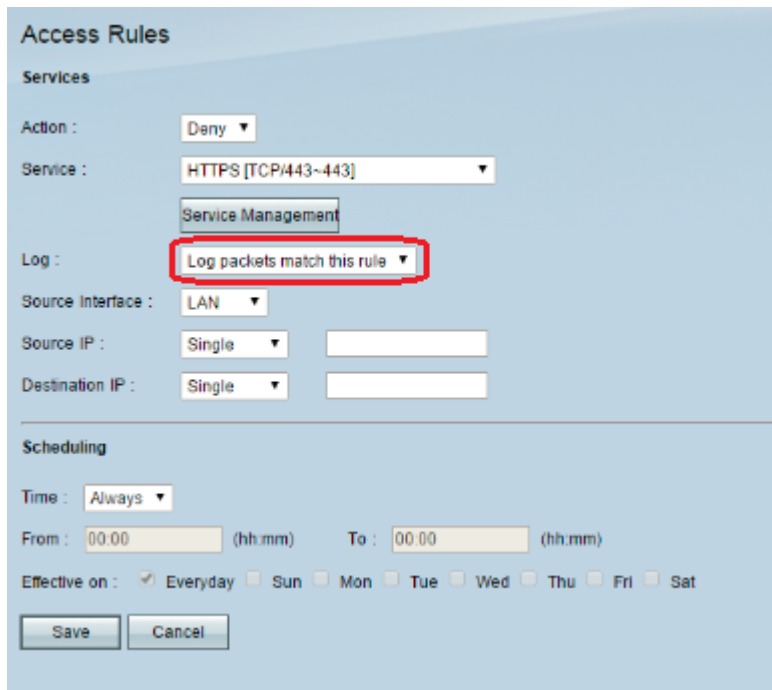
Passaggio 5. Scegliere **Nega** dall'elenco a discesa Azione per bloccare il sito Web desiderato.



Passaggio 6. Selezionare **HTTPS [TCP/443~443]** dall'elenco a discesa Servizio mentre viene bloccato un URL HTTPS.



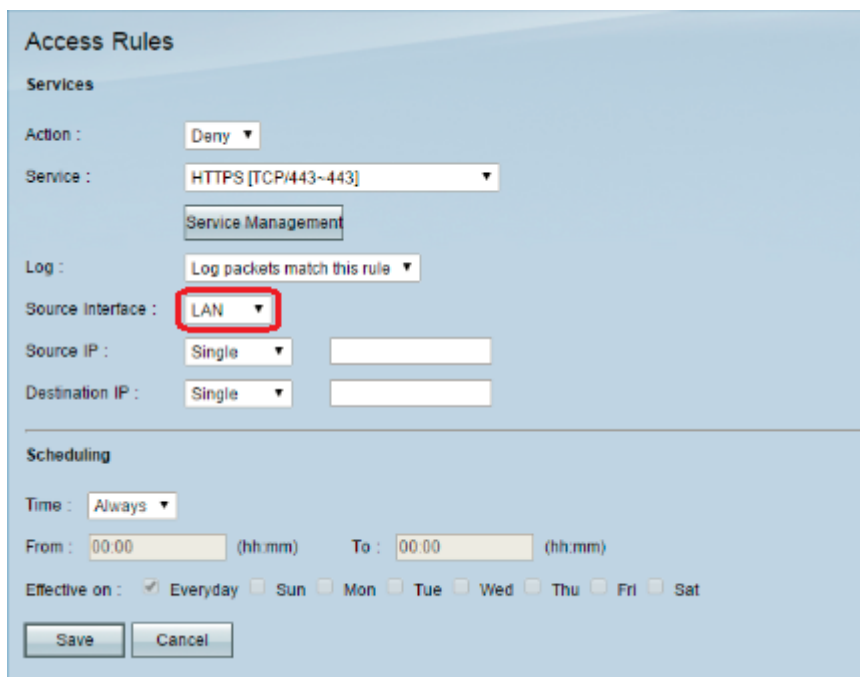
Passaggio 7. Scegliere l'opzione desiderata per Log Management dall'elenco a discesa Log.



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' dropdown is highlighted with a red box and set to 'Log packets match this rule'. The 'Source Interface' is 'LAN'. The 'Scheduling' section shows 'Time' as 'Always', 'From' and 'To' times as '00:00', and 'Effective on' checked for 'Everyday'.

- Registra pacchetti corrispondenti a questa regola - registra i pacchetti bloccati.
- Not log: non registra alcun pacchetto.

Passaggio 8. Selezionare **LAN** dall'elenco a discesa Source Interface (Interfaccia di origine) in quanto è necessario bloccare la richiesta URL che proviene dall'interfaccia LAN del router.



The screenshot shows the 'Access Rules' configuration interface. The 'Source Interface' dropdown menu is highlighted with a red box and set to 'LAN'. Other settings are the same as in the previous screenshot.

Passaggio 9. Selezionare l'opzione desiderata dall'elenco a discesa Source IP (IP origine). Immettere quindi gli indirizzi IP dei computer a cui non è consentito accedere al sito Web:

·Single: la regola blocca i pacchetti da un singolo indirizzo IP nell'interfaccia LAN.

·Intervallo: la regola blocca i pacchetti da un intervallo di indirizzi IP (solo IPv4) nell'interfaccia LAN. Immettere il primo indirizzo IP dell'intervallo nel primo campo, quindi immettere l'indirizzo IP finale nel secondo campo.

·ANY: la regola viene applicata a tutti gli indirizzi IP dell'interfaccia LAN.

Passaggio 10. Selezionare l'opzione desiderata dall'elenco a discesa IP di destinazione. Immettere quindi l'indirizzo IP dell'URL che si desidera bloccare. Per individuare queste informazioni, consultare il passo 1 e il passo 2.

· Single: la regola blocca i pacchetti da un singolo indirizzo IP nell'interfaccia LAN.

· Intervallo: la regola blocca i pacchetti da un intervallo di indirizzi IP (solo IPv4) nell'interfaccia LAN. Immettere il primo indirizzo IP dell'intervallo nel primo campo, quindi

immettere l'indirizzo IP finale nel secondo campo. In genere, questa opzione non viene utilizzata in quanto talvolta risulta imprecisa e blocca altri siti Web.

Passaggio 11. Scegliere l'opzione di programmazione desiderata nella sezione Programmazione.

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' option is checked. The 'Source interface' is 'LAN', the 'Source IP' is 'Single' with the address '192.168.1.100', and the 'Destination IP' is 'Single' and empty. In the 'Scheduling' section, the 'Time' dropdown is set to 'Always' and is highlighted with a red box. Below it, the 'From' and 'To' time fields are both set to '00:00'. 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 - questa regola blocca continuamente il sito Web.
- Intervallo: questa regola blocca il sito Web solo in un determinato orario o giorno della settimana.

Passaggio 12. Se si seleziona **Intervallo** al passo 11, inserire l'ora di inizio e di fine desiderata nei campi *Da* e *A*.

This screenshot is similar to the previous one but with the 'Time' dropdown set to 'Interval', also highlighted with a red box. The 'From' time is set to '01:30' and the 'To' time is set to '03:30', both fields also highlighted with a red box. The 'Effective on' section remains the same with 'Everyday' checked. 'Save' and 'Cancel' buttons are at the bottom.

Passaggio 13. Se si seleziona **Intervallo** al passaggio 11, selezionare i giorni desiderati in cui si desidera bloccare il sito Web oppure selezionare la casella di controllo **Ogni giorno** per

bloccare il sito Web ogni giorno.

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 : Interval ▾

From : 01:30 (hh:mm) To : 03:30 (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel

Passaggio 14. Fare clic su **Save** per salvare le impostazioni. Il sito Web specificato verrà bloccato.

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 : Interval ▾

From : 01:30 (hh:mm) To : 03:30 (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel

Ripetere i [passaggi](#) da 1 a 15 per bloccare altri URL.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).