

Bloquer l'accès HTTPS pour un site particulier sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Le protocole HTTPS (Hyper Text Transfer Protocol Secure) est une combinaison du protocole HTTP (Hyper Text Transfer Protocol) et du protocole SSL/TLS pour assurer une communication chiffrée ou sécurisée.

Ce document explique comment empêcher les utilisateurs d'accéder aux sites ou URL https désirés. Cela permettra à l'utilisateur de bloquer les sites malveillants indésirables ou connus pour des raisons de sécurité et d'autres raisons telles que le contrôle parental.

Périphériques pertinents

- RV016
- RV042
- RV042G
- RV082

Version du logiciel

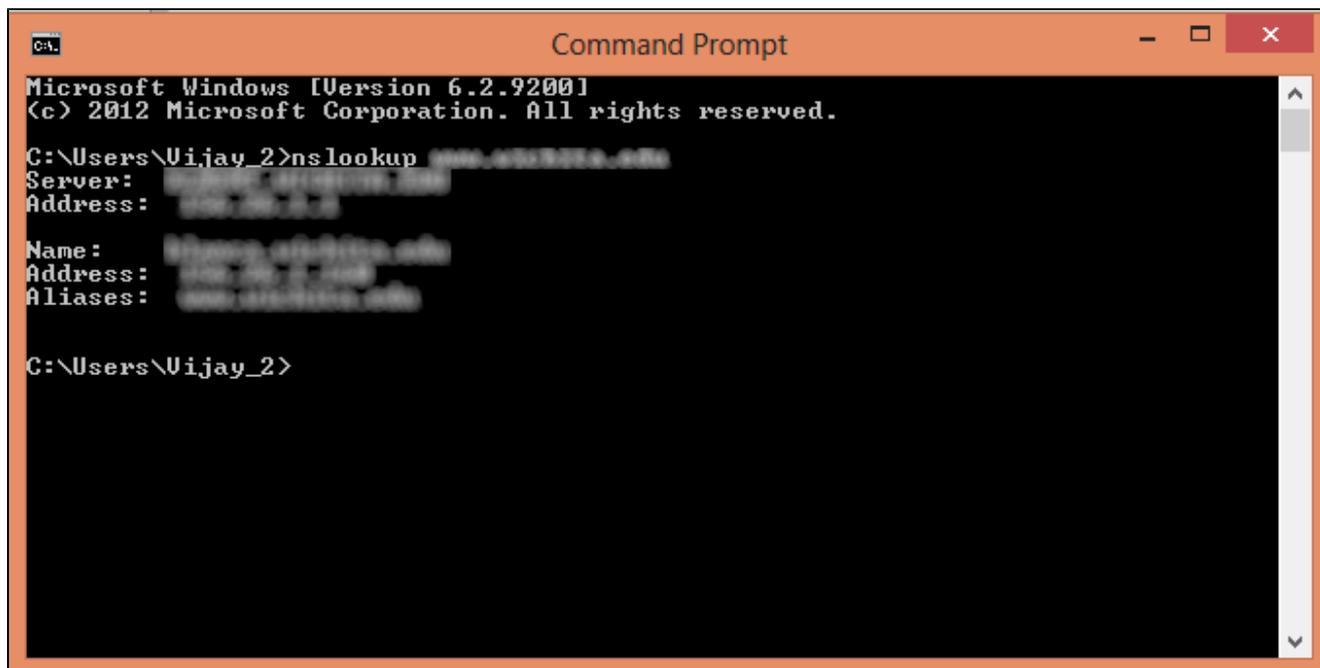
- 4.2.2.08

Bloquer l'accès HTTPS

Vous devez trouver l'adresse IP du site Web particulier que vous souhaitez bloquer. Pour ce faire, suivez les étapes 1 et 2 ci-dessous.

Étape 1. Sur votre PC, ouvrez l'invite de commande en sélectionnant Démarrer > Exécuter. Tapez ensuite cmd dans le champ Open. (Sous Windows 8, tapez simplement cmd dans l'écran Démarrer.)

Étape 2. Dans la fenêtre Invite de commandes, entrez nslookup <space> URL. L'URL est le site Web que vous souhaitez bloquer. Par exemple, si vous souhaitez bloquer le site Web « www.example.com », vous devez saisir :
nslookup www.example.com.



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

C:\Users\Uijay_2>nslookup www.example.com
Server: [redacted]
Address: [redacted]

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

C:\Users\Uijay_2>
```

Les champs suivants s'affichent :

- Server : affiche le nom du serveur DNS qui fournit des informations au routeur.
- Address : affiche l'adresse IP du serveur DNS qui fournit des informations au routeur.
- Name : affiche le nom du serveur qui héberge le site Web que vous avez entré à l'étape 2.
- Address : affiche l'adresse IP du serveur qui héberge le site Web que vous avez entré à l'étape 2.
- Alias : affiche le nom de domaine complet (FQDN) du serveur qui héberge le site Web que vous avez entré à l'étape 2.

L'adresse du serveur du site Web est ce dont nous avons besoin.

Étape 3. Connectez-vous à l'utilitaire de configuration du routeur pour choisir Firewall > Access Rules. La page Access Rule s'ouvre :



Étape 4. Cliquez sur Add pour ajouter une nouvelle règle. La fenêtre Access Rules s'affiche :



Étape 5. Choisissez Deny dans la liste déroulante Action pour bloquer le site Web souhaité.

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

Étape 6. Sélectionnez HTTPS [TCP/443~443] dans la liste déroulante Service, car nous bloquons une URL HTTPS.

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

Étape 7. Sélectionnez l'option souhaitée pour la Gestion des journaux dans la liste déroulante Journal.

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

- Consigner les paquets qui correspondent à cette règle — Consigner les paquets qui sont bloqués.

- Not log : ne consigne aucun paquet.

Étape 8. Choisissez LAN dans la liste déroulante Source Interface car nous devons bloquer la requête d'URL qui proviendra de l'interface LAN des routeurs.

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

Étape 9. Sélectionnez l'option souhaitée dans la liste déroulante Source IP. Saisissez ensuite la ou les adresses IP de la ou des machines qui ne sont pas autorisées à accéder au site Web :

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 : la règle bloque les paquets à partir d'une adresse IP unique dans l'interface LAN.
- Range : la règle bloque les paquets d'une plage d'adresses IP (IPv4 uniquement) dans l'interface LAN. Entrez la première adresse IP de la plage dans le premier champ, puis l'adresse IP finale dans le second champ.
- ANY : la règle s'applique à toutes les adresses IP de l'interface LAN.

Étape 10. Sélectionnez l'option souhaitée dans la liste déroulante Destination IP. Saisissez ensuite l'adresse IP de l'URL que vous souhaitez bloquer. Reportez-vous aux étapes 1 et 2 pour trouver ces informations.

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 : la règle bloque les paquets à partir d'une adresse IP unique dans l'interface LAN.
- Range : la règle bloque les paquets d'une plage d'adresses IP (IPv4 uniquement) dans l'interface LAN. Entrez la première adresse IP de la plage dans le premier champ, puis l'adresse IP finale dans le second champ. Généralement, cette option n'est pas utilisée car elle peut parfois être inexacte et bloquer d'autres sites Web.

Étape 11. Sélectionnez l'option de planification souhaitée dans la section Planification.

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

- Toujours — Cette règle bloque le site Web tout le temps.
- Intervalle — Cette règle ne bloque le site Web qu'à une heure ou un jour précis de la semaine.

Étape 12. Si vous sélectionnez Intervalle à l'étape 11, entrez les heures de début et de fin souhaitées dans les champs From et To.

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

Étape 13. Si vous sélectionnez Interval à l'étape 11, cochez le(s) jour(s) souhaité(s) où vous souhaitez bloquer le site Web ou cochez la case Everyday pour bloquer le site Web chaque jour.

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

Étape 14. Cliquez sur Save pour enregistrer les paramètres. Le site Web spécifié sera bloqué.

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

Répétez les [étapes 1](#) à 15 pour bloquer d'autres URL.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.