HTTPS-toegang blokkeren voor een bepaalde site op RV016-, RV042-, RV042G- en RV082 VPNrouters

Doel

Hyper Text Transfer Protocol Secure (HTTPS) is een combinatie van Hyper Text Transfer Protocol (HTTP) met SSL/TLS-protocol voor versleutelde communicatie of beveiligde communicatie.

Dit document legt uit hoe u kunt voorkomen dat gebruikers toegang krijgen tot de gewenste httpswebsites of URL's. Dit zal de gebruiker helpen om ongewenste of bekende kwaadaardige sites te blokkeren voor veiligheid en andere redenen zoals ouderlijk toezicht.

Toepasselijke apparaten

• RV016 •RV042 • RV042G • RV082

Softwareversie

•4.2.2.08

HTTPS-toegang blokkeren

U moet het IP-adres vinden van de specifieke website die u wilt blokkeren. Volg daartoe de onderstaande stappen 1 en 2.

Stap 1. Open op uw pc de opdrachtprompt **Start > Run**. Typ vervolgens **cmd** in het veld Openen. (Typ in Windows 8 alleen **cmd** in het **Beginscherm**.)

Stap 2. Voer in het venster Opdrachtprompt **nslookup** <space> URL in. De URL is de website die u wilt blokkeren. Als u bijvoorbeeld de website "www.example.com" wilt blokkeren, voert u het volgende in:

nslookup www.example.com.



De volgende velden worden weergegeven:

· Server â€" Toont de naam van de DNS server die informatie aan de router verstrekt.

· Adres â€" Hier wordt het IP-adres van de DNS-server weergegeven dat informatie aan de router geeft.

· Naam $\hat{a} \in$ " Hier wordt de naam weergegeven van de server waarop de website wordt gehost die u in Stap 2 hebt ingevoerd.

· Adres $\hat{a} \in$ " Hier wordt het IP-adres weergegeven van de server waarop de website wordt gehost die u in stap 2 hebt ingevoerd.

· Aliassen $\hat{a} \in$ " Hier wordt de volledig gekwalificeerde domeinnaam (FQDN) weergegeven van de server waarop de website wordt gehost die u in Stap 2 hebt ingevoerd.

Het serveradres van de website is wat we nodig hebben.

Stap 3. Log in het hulpprogramma Routerconfiguratie om **Firewall > toegangsregels** te kiezen. De pagina *Toegangsregels* wordt geopend:

| Access F | Rules IPv6 | | | | | | | | | |
|----------|---------------|------------|-----------------|---------------------|--------|-------------|----------|---------------|----------|--------|
| | | | | | | | Item 1-3 | of 3 Rows per | r page : | 5 🔻 |
| Priority | Enable | Action | Service | Source Interface | Source | Destination | Time | Day | | Delete |
| | | Allow | All Traffic [1] | LAN | Any | Any | Always | | | |
| | 1 | Deny | All Traffic [1] | WAN1 | Any | Any | Always | | | |
| | | Deny | All Traffic [1] | WAN2 | Any | Any | Always | | | |
| Add | Restore to I | Default Ru | les | | | | | Page 1 | of 1 | |

Stap 4. Klik op Add om een nieuwe regel toe te voegen. Het venster Toegangsregels verschijnt:

| Access Rules | | | | | | | | | |
|--------------|---|--|--|---|---|--|---|--|--|
| IPv6 | | | | | | | | | |
| | | | | | | Item 1-3 | of 3 Rows pe | r page : | 5 🔻 |
| Enable | Action | Service | Source Interface | Source | Destination | Time | Day | | Delete |
| V | Allow | All Traffic [1] | LAN | Any | Any | Always | | | |
| 4 | Deny | All Traffic [1] | WAN1 | Any | Any | Always | | | |
| | Deny | All Traffic [1] | WAN2 | Any | Any | Always | | | |
| estore to C | Default Ru | les | | | | | Page 1 | • of 1 | |
| | IPv6 Enable Ø Ø estore to 0 | Iles IPv6 IPv6 Action Allow Ony Deny store to Default Ru | Iles IPv6 IPv6 IPv6 Action Service Allow All Traffic [1] Deny All Traffic [1] Deny All Traffic [1] Allow Compared to Default Rules | Iles IPv6 IPv6 IPv6 Action Service Source Interface Allow All Traffic [1] LAN Deny All Traffic [1] WAN1 Deny All Traffic [1] WAN2 estore to Default Rules | IPv6 IPv6 Enable Action Service Source Interface Interface Source Image: Allow All Traffic [1] LAN Image: Deny All Traffic [1] WAN1 Deny All Traffic [1] WAN2 Image: Deny All Traffic [1] WAN2 Any Source Source Image: Deny All Traffic [1] WAN2 Image: Deny All Traffic [1] WAN2 | Iles IPv6 IPv6 Source Source Destination Enable Action Service Source Destination Image: Action Allow All Traffic [1] LAN Any Any Image: Action Deny All Traffic [1] WAN1 Any Any Image: Deny All Traffic [1] WAN2 Any Any Image: Deny All Traffic [1] WAN2 Any Any Image: Deny All Traffic [1] WAN2 Any Any | Iles Item 1-3 Item 1-3 Enable Action Source Destination Time Colspan="5">Allow All Traffic [1] LAN Any Always Colspan="5">Deny All Traffic [1] VAN1 Any Always Colspan="5">Obeny All Traffic [1] VAN2 Any Always Colspan="5">Deny All Traffic [1] VAN2 Any Always Image: colspan="5">Image: colspan="5">Image: colspan="5">Image: colspan="5" | Iles Item 1-3 of 3 Rows pe Item 1-3 of 3 Rows pe Item 1-3 of 3 Rows pe Enable Action Service Source Destination Time Day Image: Action Service Source Source Destination Time Day Day Image: Action All Traffic [1] LAN Any Any Always Image: Always Image: All Traffic [1] WAN1 Any Any Always Image: Always Image: Always Image: All Traffic [1] WAN2 Any Any Always Image: Always Image: Always | Iles Item 1-3 of 3 Rows per page : Item 1-3 of 3 Rows per page : Enable Action Service Source Destination Time Day Allow All Traffic [1] LAN Any Any Always Image: Source Deny All Traffic [1] WAN1 Any Any Always Deny All Traffic [1] WAN2 Any Any Always Image: Source Deny All Traffic [1] WAN2 Any Any Always |

Stap 5. Kies **Ontkennen** in de vervolgkeuzelijst Actie om de gewenste website te blokkeren.

| Access Rules | |
|--------------------|--|
| Services | |
| Action : | Deny 🔻 |
| Service : | All Traffic [TCP&UDP/1~65535] |
| | Service Management |
| Log : | Log packets match this rule 🔻 |
| Source Interface : | LAN V |
| Source IP : | Single • |
| Destination IP : | Single • |
| Scheduling | |
| Time : Always 🔻 | |
| From : 00:00 | (hh.mm) To: 00:00 (hh.mm) |
| Effective on : 🧭 E | everyday 🕘 Sun 🕘 Mon 💭 Tue 💭 Wed 💭 Thu 💭 Fri 🗔 Sat |
| Save Ca | ncel |

Stap 6. Kies **HTTPS** [**TCP/443~443**] in de vervolgkeuzelijst Service omdat we een HTTPS-URL blokkeren.

| Access Rules | | | | |
|---|-------------------------------|--|--|--|
| Services | | | | |
| Action : | Deny T | | | |
| Service : | HTTPS [TCP/443~443] | | | |
| | Service Management | | | |
| Log : | Log packets match this rule 🔻 | | | |
| Source Interface : | LAN T | | | |
| 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 | | | | |

Stap 7. Kies de gewenste optie voor het Logbeheer in de vervolgkeuzelijst Log.

| Access Rules | | | | |
|---|-------------------------------|--|--|--|
| Services | | | | |
| Action : | Deny • | | | |
| Service : | HTTPS [TCP/443~443] | | | |
| | Service Management | | | |
| Log : | Log packets match this rule 💌 | | | |
| Source Interface : | LAN V | | | |
| Source IP : | Single T | | | |
| 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 | | | | |

· Logpakketten voldoen aan deze regel $\hat{a} \in$ " logt de pakketten in die worden geblokkeerd.

· Niet log â€" Zal geen pakketten vastleggen.

Stap 8. Kies **LAN** in de vervolgkeuzelijst Source Interface omdat we het URL-verzoek moeten blokkeren dat afkomstig zal zijn van de routers LAN-interface.

| Access Rules | | |
|---|-------------------------------|--|
| Services | | |
| Action : | Deny • | |
| Service : | HTTPS [TCP/443~443] | |
| | Service Management | |
| Log : | Log packets match this rule 🔻 | |
| Source Interface : | LAN V | |
| 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 | | |

Stap 9. Kies de gewenste optie in de vervolgkeuzelijst Bron-IP. Voer vervolgens het IP-adres in van de machine(s) die geen toegang hebben tot de website:

| 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 : 🕑 E | veryday 🗌 Sun 🗌 Mon 🗍 Tue 🗍 Wed 🗍 Thu 🦳 Fri 🗌 Sat |
| Save Car | ncel |

· Enkelvoudig â€" De regel blokkeert pakketten vanaf één IP-adres in de LAN-interface.

• Bereik â€" De regel blokkeert pakketten van een reeks IP-adressen (alleen IPv4) in de LANinterface. Voer in het eerste veld het eerste IP-adres van het bereik in en voer in het tweede veld het laatste IP-adres in.

· ALLE â€" De regel is van toepassing op alle IP-adressen in de LAN-interface.

Stap 10. Kies de gewenste optie uit de vervolgkeuzelijst Bestemming IP. Voer vervolgens het IP-adres in van de URL die u wilt blokkeren. Zie Stap 1 en Stap 2 om u te helpen deze informatie te vinden.

| Access Rules | | | | |
|---|-------------------------------|--|--|--|
| Services | | | | |
| Action : | Deny T | | | |
| Service : | HTTPS [TCP/443~443] | | | |
| | Service Management | | | |
| Log : | Log packets match this rule 🔻 | | | |
| Source Interface : | LAN T | | | |
| 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 | | | | |
| | | | | |

· Enkelvoudig â€" De regel blokkeert pakketten vanaf één IP-adres in de LAN-interface.

• Bereik â€" De regel blokkeert pakketten van een reeks IP-adressen (alleen IPv4) in de LANinterface. Voer in het eerste veld het eerste IP-adres van het bereik in en voer in het tweede veld het laatste IP-adres in. Meestal wordt deze optie niet gebruikt omdat het soms onnauwkeurig zal zijn en andere websites zal blokkeren.

Stap 11. Kies de gewenste planningsoptie in het gedeelte Scheduling.

| 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 T | | | | |
| From : 00.00 (hh.mm) To : 00.00 (hh.mm) | | | | |
| Effective on : 🏾 Everyday 🗋 Sun 🗋 Mon 💭 Tue 💭 Wed 💭 Thu 💭 Fri 💭 Sat | | | | |
| Save Cancel | | | | |

· Altijd â€" Deze regel blokkeert de website voortdurend.

· Interval â€" Deze regel blokkeert de website alleen op een bepaald tijdstip of op een bepaalde dag van de week.

Stap 12. Als u **Interval** selecteert in Stap 1, voert u de gewenste begin- en eindtijd in de velden *Van* en *Tot in*.

| Access Rules | | | | |
|---|-------------------------------|--|--|--|
| Services | | | | |
| Action : | Deny • | | | |
| Service : | HTTPS [TCP/443~443] | | | |
| | Service Management | | | |
| Log : | Log packets match this rule 🔻 | | | |
| Source Interface : | LAN T | | | |
| Source IP : | Single • 192.168.1.100 | | | |
| Destination IP : | Single T | | | |
| 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 | | | | |

Stap 13. Als u **Interval** selecteert bij Stap 11, kruis dan de gewenste dag(en) aan waarop u de website wilt blokkeren of kruis het **vakje** Elke dag aan om de website te blokkeren.

| Access Rules | | | | |
|---|-------------------------------|--|--|--|
| Services | | | | |
| Action : | Deny 🔻 | | | |
| Service : | HTTPS [TCP/443~443] | | | |
| | Service Management | | | |
| Log : | Log packets match this rule 🔻 | | | |
| Source Interface : | LAN T | | | |
| Source IP : | Single • 192.168.1.100 | | | |
| Destination IP : | Single T | | | |
| 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 | | | | |

Stap 14. Klik op **Opslaan** om de instellingen op te slaan. De gespecificeerde website wordt geblokkeerd.

| Access Rules | | | | | |
|---|-------------------------------|--|--|--|--|
| Services | | | | | |
| Action : | Deny T | | | | |
| Service : | HTTPS [TCP/443~443] | | | | |
| | Service Management | | | | |
| Log : | Log packets match this rule 🔻 | | | | |
| Source Interface : | LAN T | | | | |
| 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 | | | | | |

Herstelt <u>Stap 1</u> tot Stap 15 om meer URL's te blokkeren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.