# HTTPS-toegang blokkeren voor een bepaalde site op RV016-, RV042-, RV042G- en RV082 VPN-routers

## 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 https-websites 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
â€¢RV042
· RV042G
· RV082

## Softwareversie

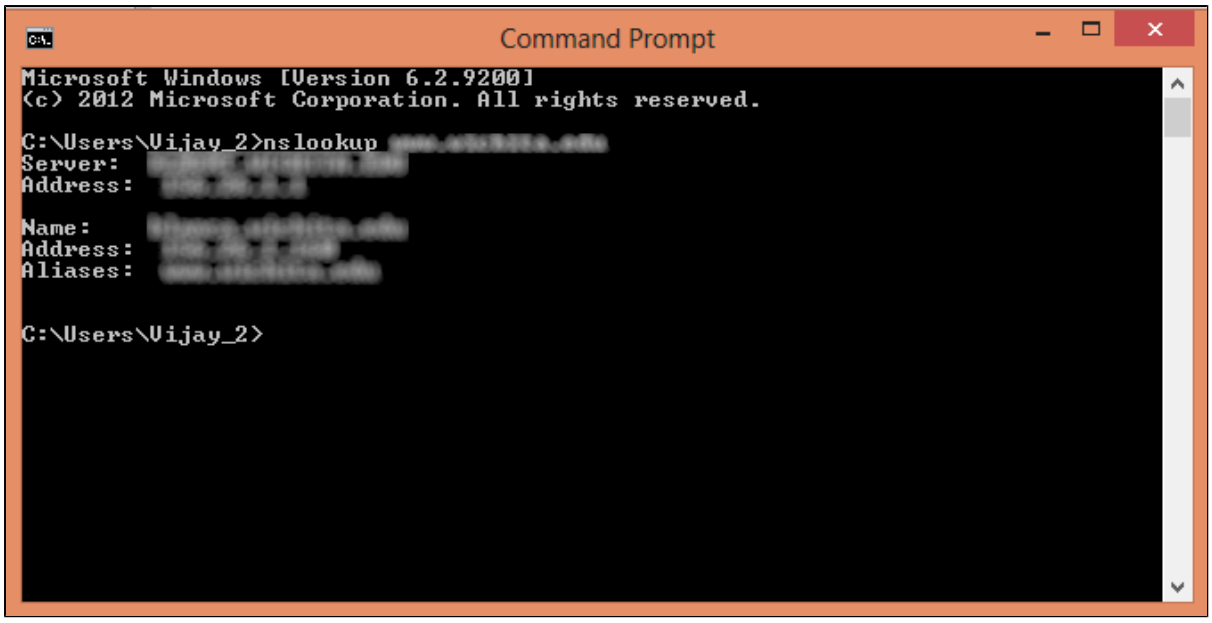
â€¢4.2.2.08

## 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.

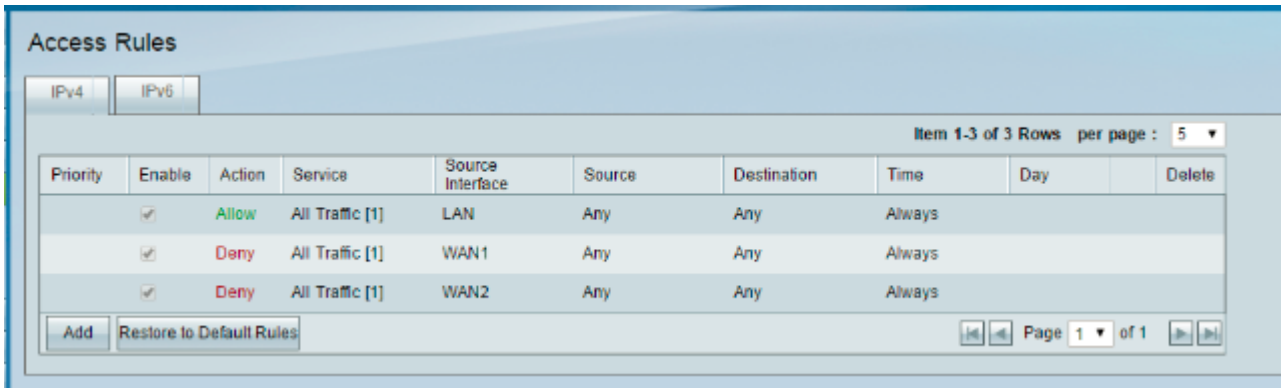
· Naam â€" Hier wordt de naam weergegeven van de server waarop de website wordt gehost die u in Stap 2 hebt ingevoerd.

· Adres â€" Hier wordt het IP-adres weergegeven van de server waarop de website wordt gehost die u in stap 2 hebt ingevoerd.

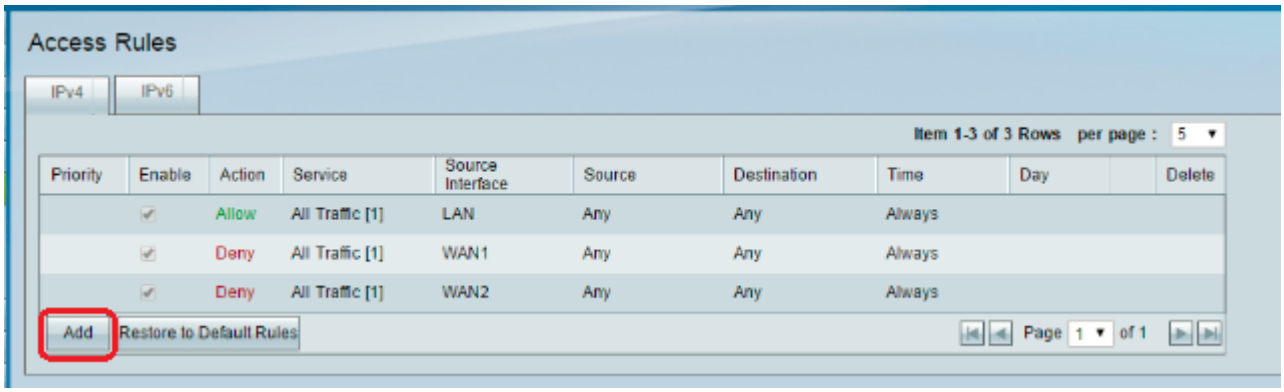
· Aliassen â€" Hier wordt de volledig gekwalificeerde domeinnaam (FQDN) weergegeven van de server waarop de website wordt gehost die u in Stap 2 hebt ingevoerd.

Het serveradres van de website is wat we nodig hebben.

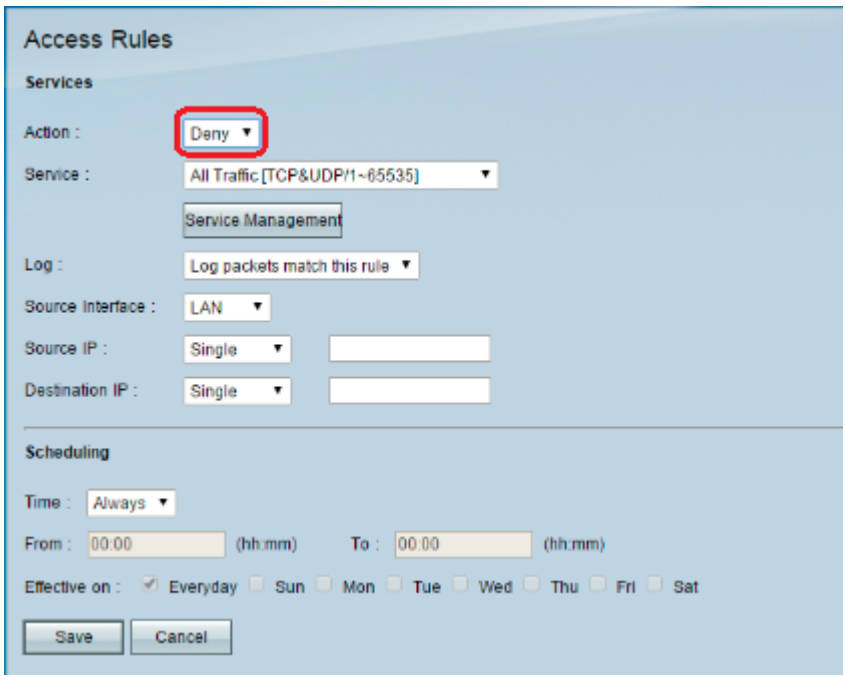
Stap 3. Log in het hulpprogramma Routerconfiguratie om **Firewall > toegangsregels** te kiezen. De pagina *Toegangsregels* wordt geopend:



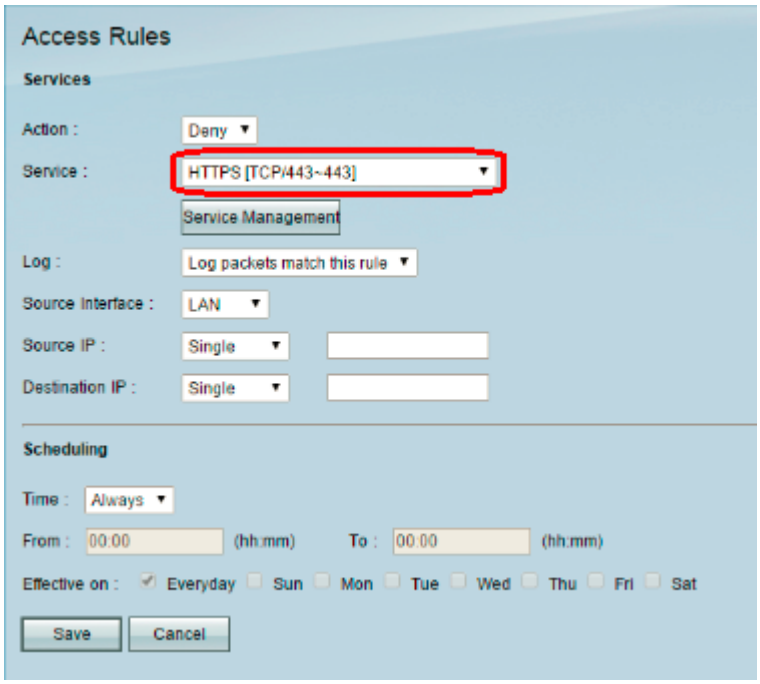

Stap 4. Klik op **Add** om een nieuwe regel toe te voegen. Het venster *Toegangsregels* verschijnt:



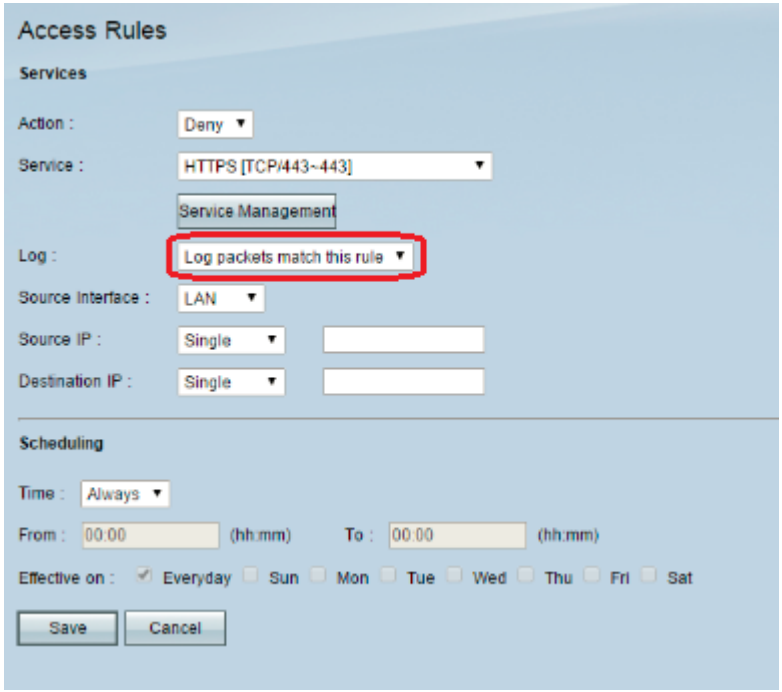

Stap 5. Kies **Ontkennen** in de vervolgkeuzelijst Actie om de gewenste website te blokkeren.




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



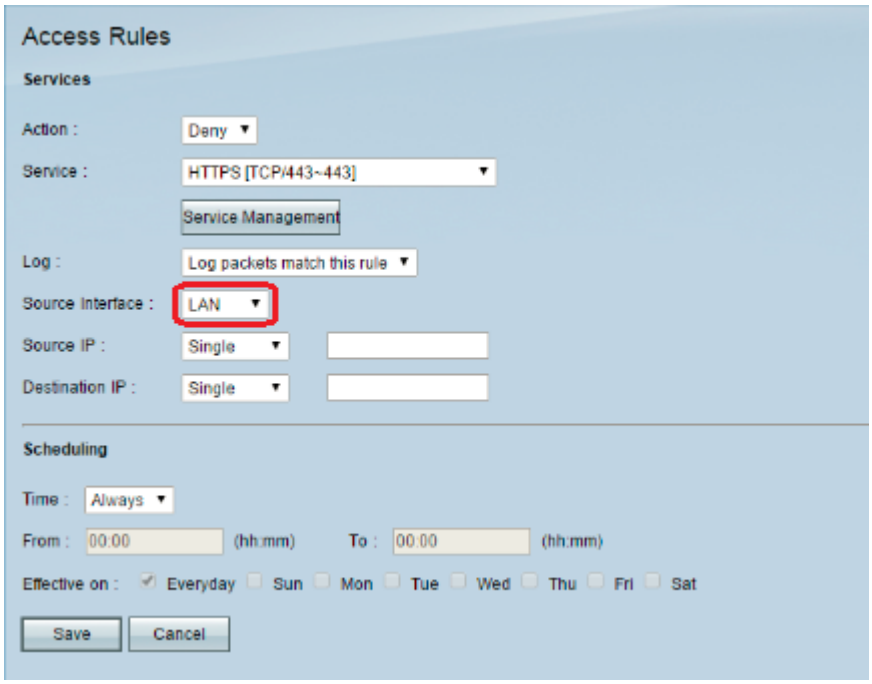

Stap 7. Kies de gewenste optie voor het Logbeheer in de vervolgkeuzelijst Log.



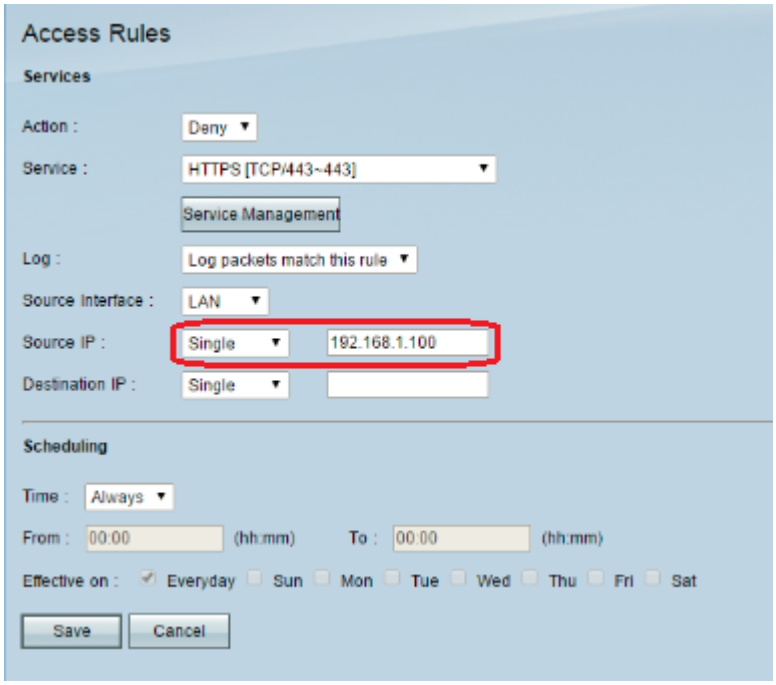

· Logpakketten voldoen aan deze regel â€" logt de pakketten in die worden geblokkeerd.

· 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.




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:

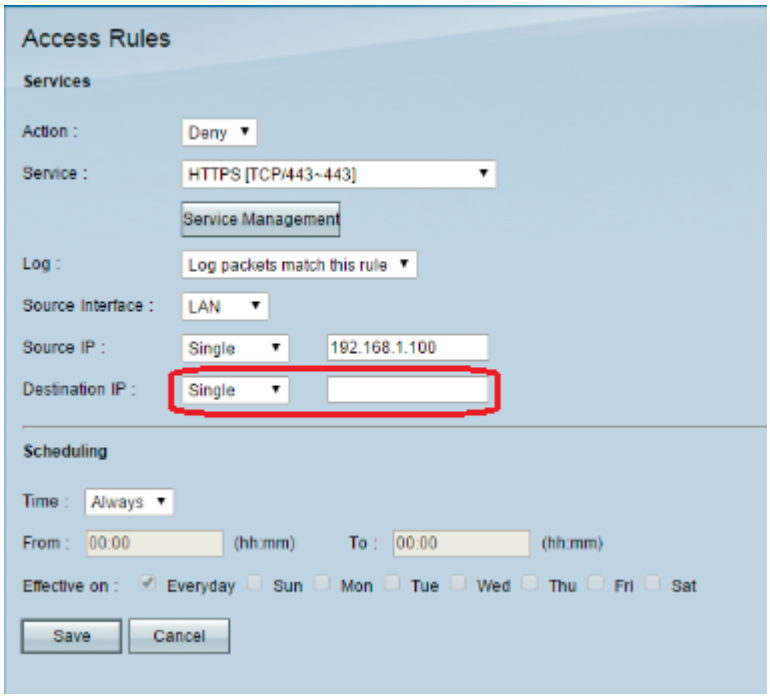



· Enkelvoudig â€" De regel blokkeert pakketten vanaf één IP-adres in de LAN-interface.

· Bereik â€" De regel blokkeert pakketten van een reeks IP-adressen (alleen IPv4) in de LAN-interface. 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.

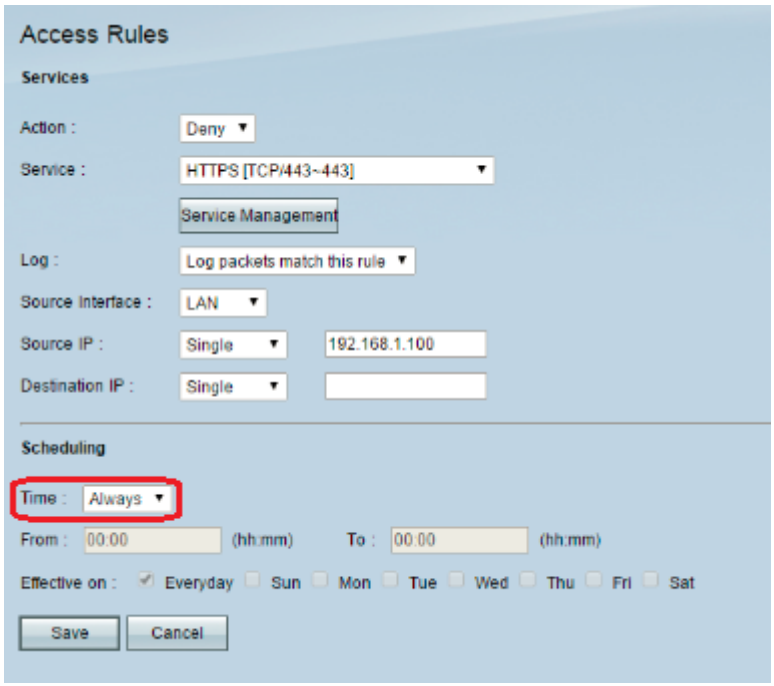
Stap 10. Kies de gewenste optie uit de vervolgkeuzelijst Bestemming IP. Voer vervolgens het IP-adres in van de URL die u wilt blokkeren. Zie Stap 1 en Stap 2 om u te helpen deze informatie te vinden.




· 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 LAN-interface. 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.

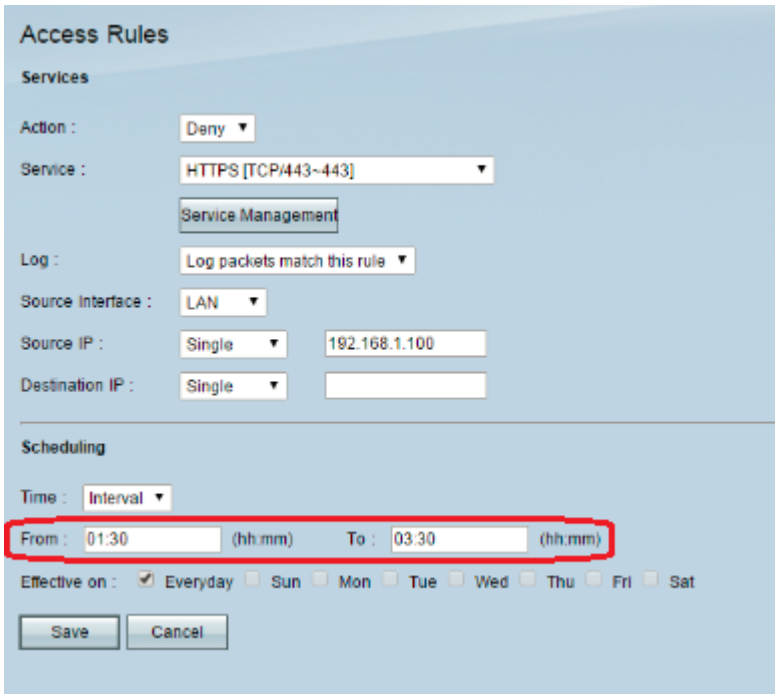
Stap 11. Kies de gewenste planningsoptie in het gedeelte Scheduling.



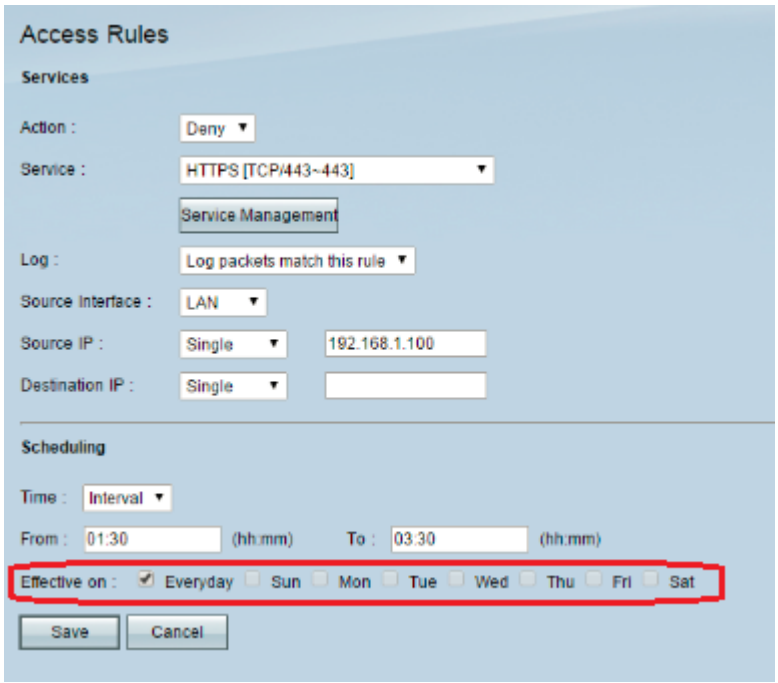

· Altijd â€" Deze regel blokkeert de website voortdurend.

· 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*.




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.




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


Herstelt Stap 1 tot Stap 15 om meer URLâ€™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.