Blockieren des HTTPS-Zugriffs für einen bestimmten Standort auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Hyper Text Transfer Protocol Secure (HTTPS) ist eine Kombination aus Hyper Text Transfer Protocol (HTTP) und SSL/TLS-Protokoll, um eine verschlüsselte oder sichere Kommunikation bereitzustellen.

In diesem Dokument wird erläutert, wie Benutzer am Zugriff auf gewünschte HTTPS-Websites oder URLs gehindert werden können. Dies hilft dem Benutzer, unerwünschte oder bekannte schädliche Websites aus Sicherheits- und anderen Gründen wie der Kindersicherung zu blockieren.

Unterstützte Geräte

RV016
â€¢RV042
ãƒ» RV042G
RV082

Software-Version

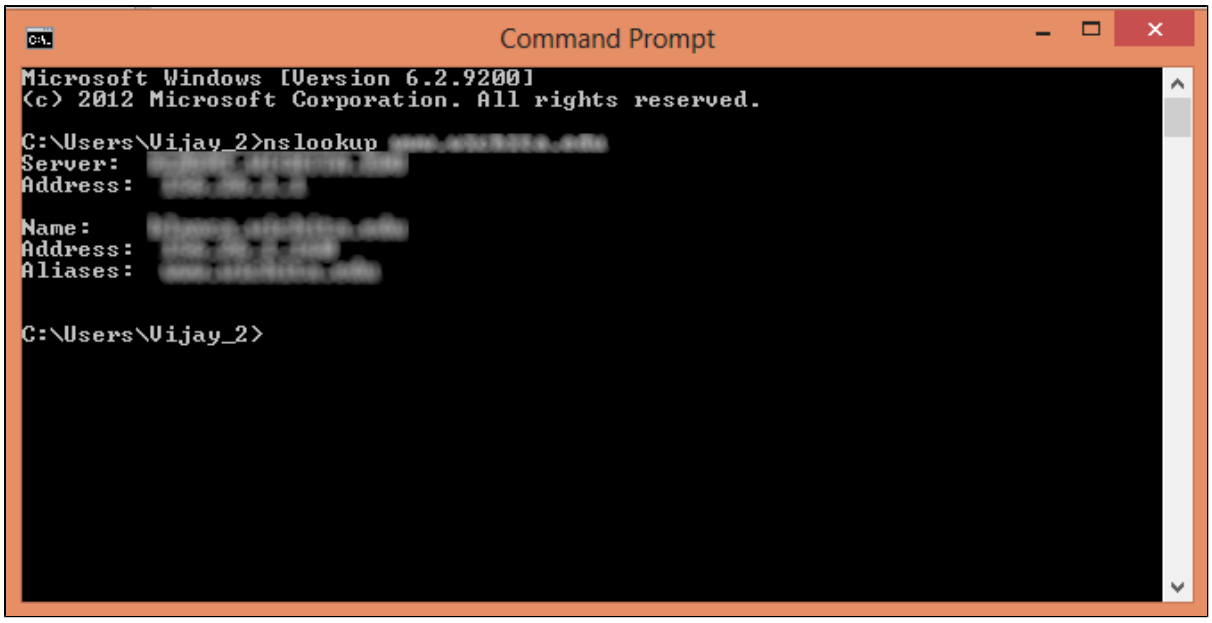
â€¢4.2.2.08

HTTPS-Zugriff blockieren

Sie müssen die IP-Adresse der Website finden, die Sie blockieren möchten. Führen Sie dazu bitte die unten aufgeführten Schritte 1 und 2 aus.

Schritt 1: Öffnen Sie auf Ihrem PC die Eingabeaufforderung mit **Start > Ausführen**. Geben Sie dann **cmd** in das Feld Öffnen ein. (Geben Sie in Windows 8 einfach **cmd** im **Startbildschirm ein**.)

Schritt 2: Geben Sie im Fenster Eingabeaufforderung die URL **nslookup**<space> ein. Die URL ist die Website, die Sie blockieren möchten. Wenn Sie beispielsweise die Website "www.example.com" blockieren möchten, geben Sie Folgendes ein:
nslookup www.example.com.



Folgende Felder werden angezeigt:

ãƒ» Server â€" Zeigt den Namen des DNS-Servers an, der dem Router Informationen bereitstellt.

ãƒ» Adresse - Zeigt die IP-Adresse des DNS-Servers an, der Informationen an den Router liefert.

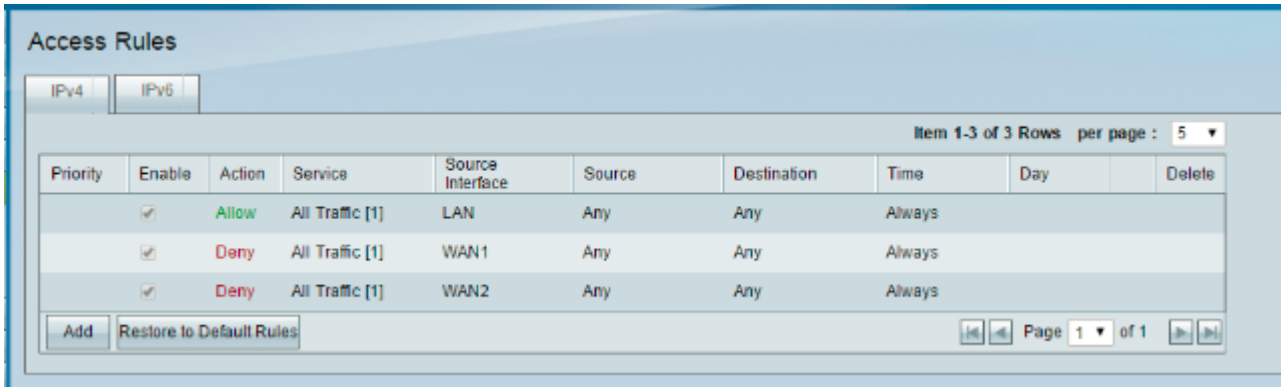
ãƒ» Name - Zeigt den Namen des Servers an, der die Website hostet, die Sie in Schritt 2 eingegeben haben.

ãƒ» Adresse â€" Zeigt die IP-Adresse des Servers an, der die Website hostet, die Sie in Schritt 2 eingegeben haben.

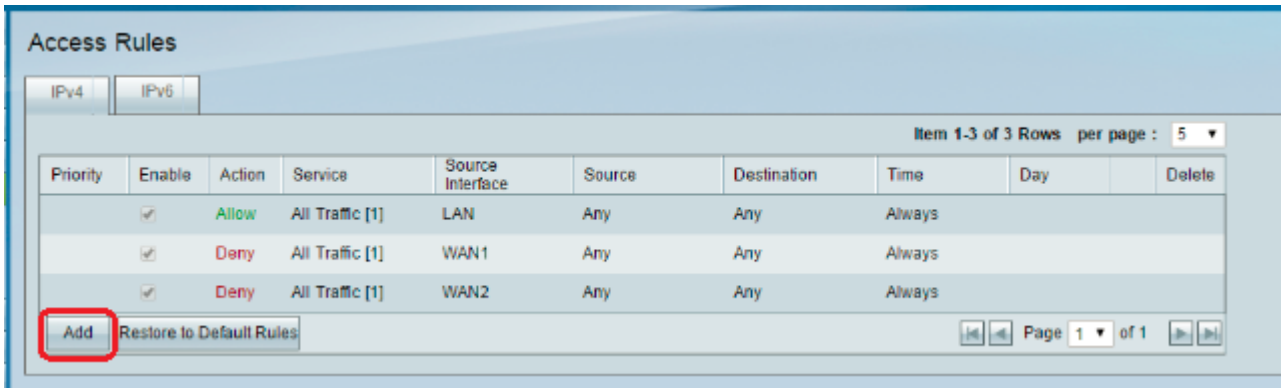
ãƒ» Aliase â€" Zeigt den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Servers an, der die in Schritt 2 eingegebene Website hostet.

Die Server-Adresse der Website ist, was wir brauchen.

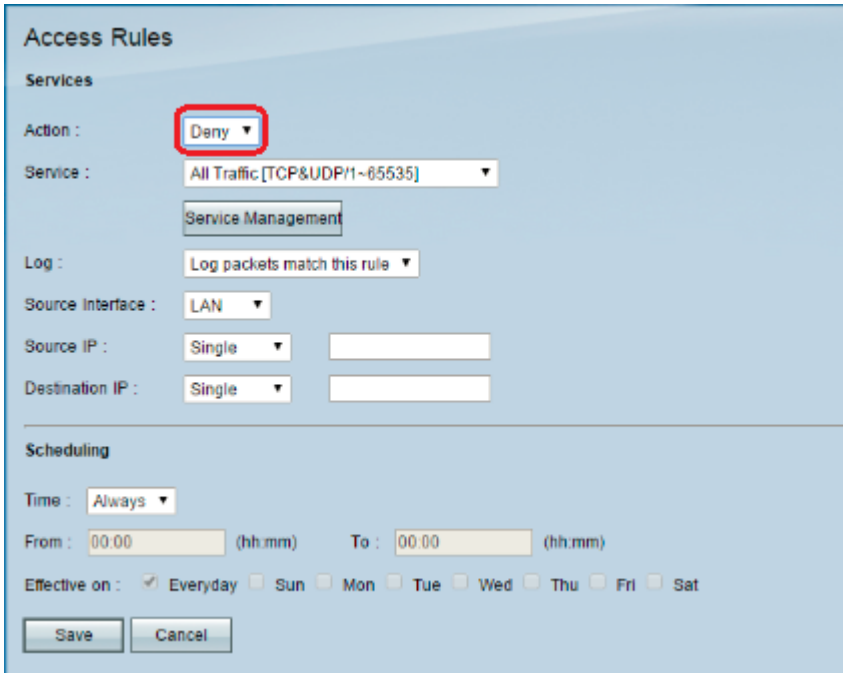
Schritt 3: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **Firewall > Access Rules**. Die Seite *Zugriffsregel* wird geöffnet:



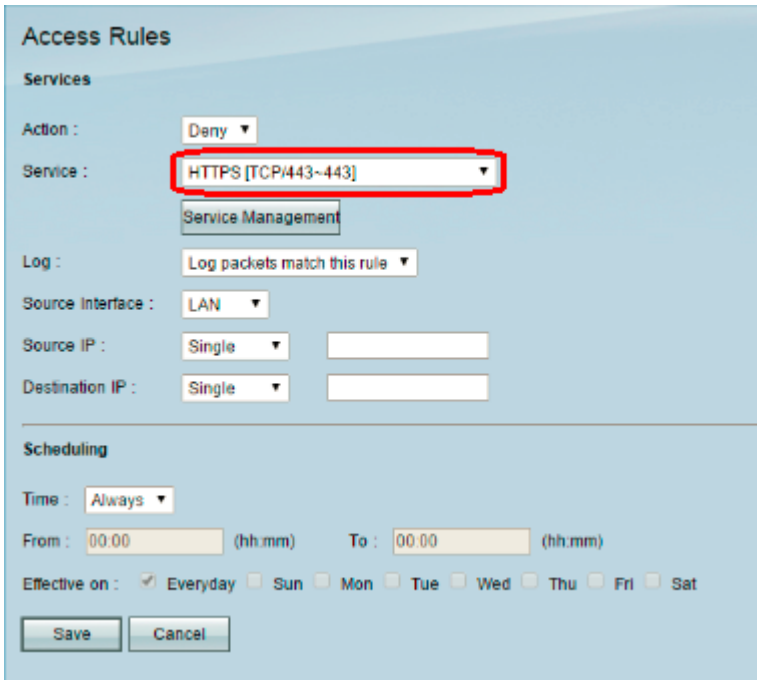
Schritt 4: Klicken Sie auf **Hinzufügen**, um eine neue Regel hinzuzufügen. Das Fenster *Access* Rules (Zugriffsregeln) wird angezeigt:



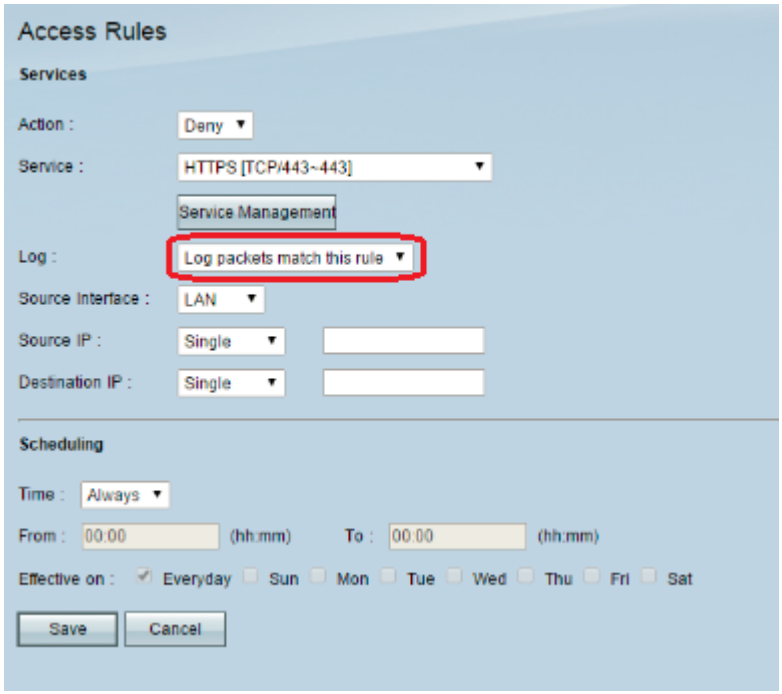
Schritt 5: Wählen Sie **Verweigern** aus der Dropdown-Liste Aktion, um die gewünschte Website zu blockieren.



Schritt 6: Wählen Sie **HTTPS [TCP/443~443]** aus der Dropdown-Liste "Service" aus, da eine HTTPS-URL blockiert wird.



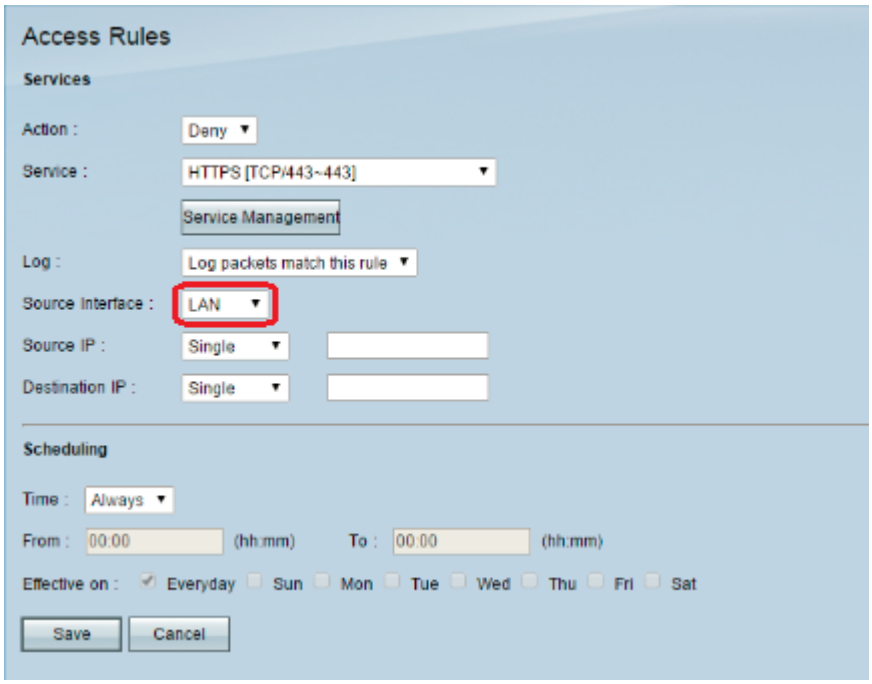
Schritt 7. Wählen Sie die gewünschte Option für die Protokollverwaltung aus der Dropdown-Liste aus.



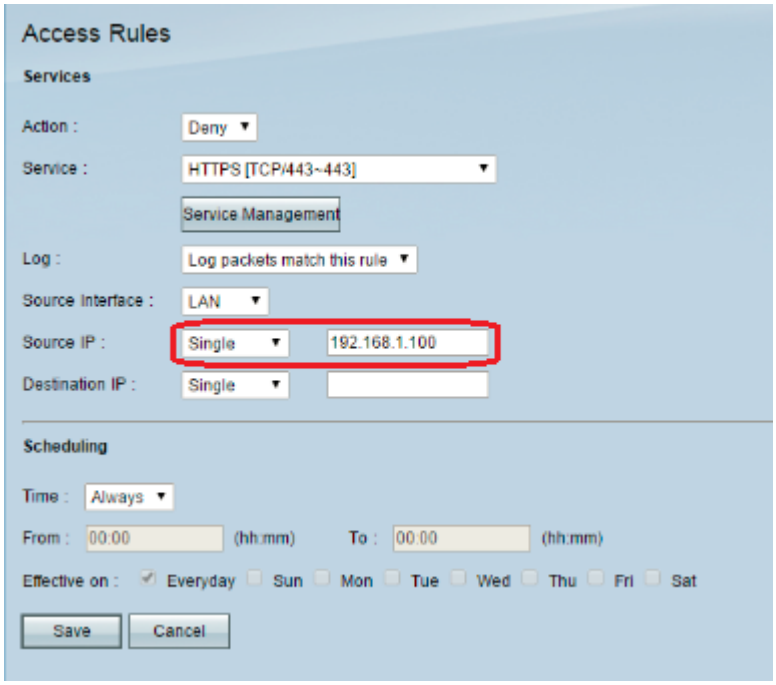
ãƒ» Protokollpakete stimmen mit dieser Regel überein: Die blockierten Pakete werden protokolliert.

ãƒ» Keine Protokollierung - Keine Pakete werden protokolliert.

Schritt 8: Wählen Sie **LAN** aus der Dropdown-Liste Source Interface (Quellschnittstelle) aus, da die URL-Anforderung blockiert werden muss, die von der LAN-Schnittstelle des Routers stammt.



Schritt 9. Wählen Sie die gewünschte Option aus der Dropdown-Liste "Source IP" aus. Geben Sie dann die IP-Adresse(n) der Geräte ein, die nicht auf die Website zugreifen dürfen:

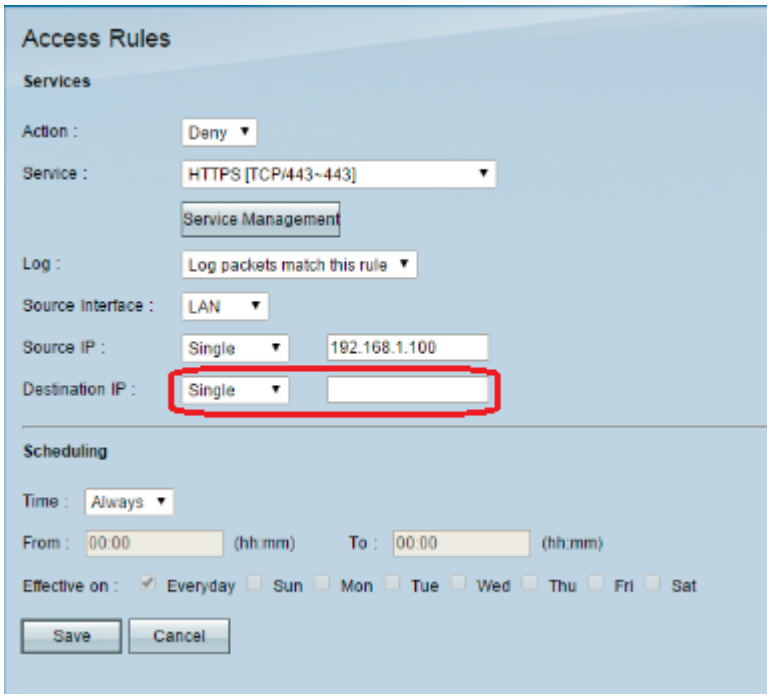


ãƒ» Single - Die Regel blockiert Pakete von einer einzigen IP-Adresse in der LAN-Schnittstelle.

ãƒ» Bereich - Die Regel blockiert Pakete aus einem IP-Adressbereich (nur IPv4) der LAN-Schnittstelle. Geben Sie die erste IP-Adresse des Bereichs in das erste Feld ein, und geben Sie dann die letzte IP-Adresse in das zweite Feld ein.

ãƒ» ANY - Die Regel gilt für alle IP-Adressen in der LAN-Schnittstelle.

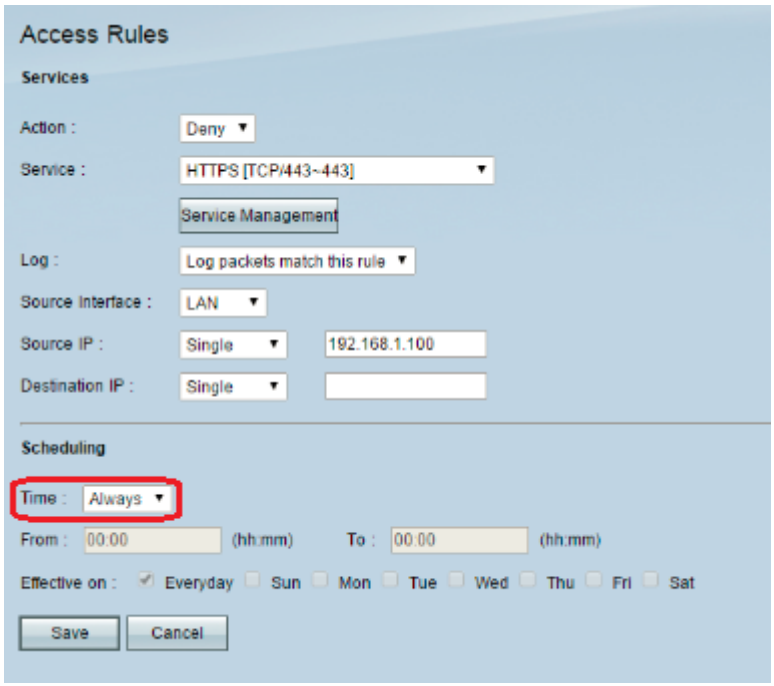
Schritt 10. Wählen Sie die gewünschte Option aus der Dropdown-Liste Destination IP (Ziel-IP) aus. Geben Sie dann die IP-Adresse der URL ein, die Sie blockieren möchten. In den Schritten 1 und 2 finden Sie die entsprechenden Informationen.



ãƒ» Single - Die Regel blockiert Pakete von einer einzigen IP-Adresse in der LAN-Schnittstelle.

ãƒ» Bereich - Die Regel blockiert Pakete aus einem IP-Adressbereich (nur IPv4) der LAN-Schnittstelle. Geben Sie die erste IP-Adresse des Bereichs in das erste Feld ein, und geben Sie dann die letzte IP-Adresse in das zweite Feld ein. Normalerweise wird diese Option nicht verwendet, da sie manchmal ungenau ist und andere Websites blockiert.

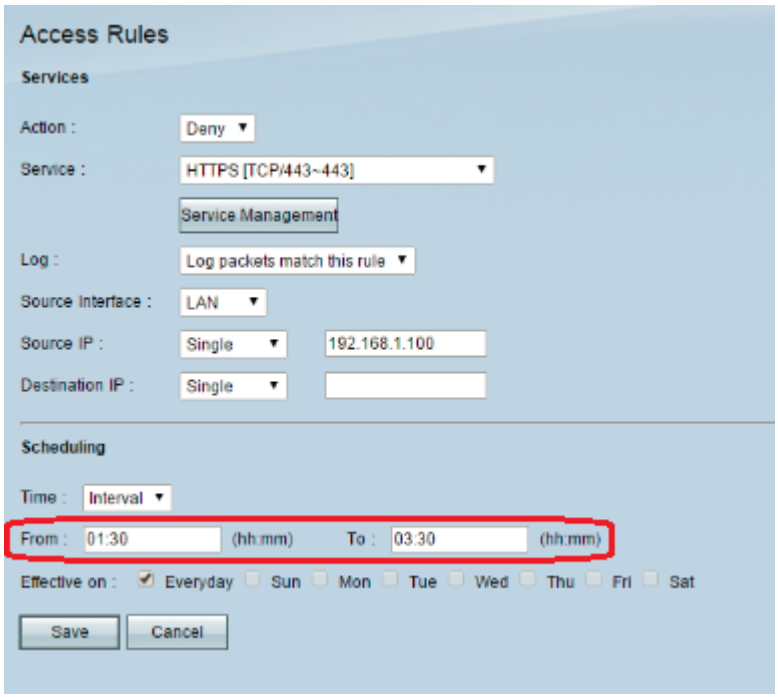
Schritt 11. Wählen Sie im Abschnitt "Planung" die gewünschte Planungsoption aus.



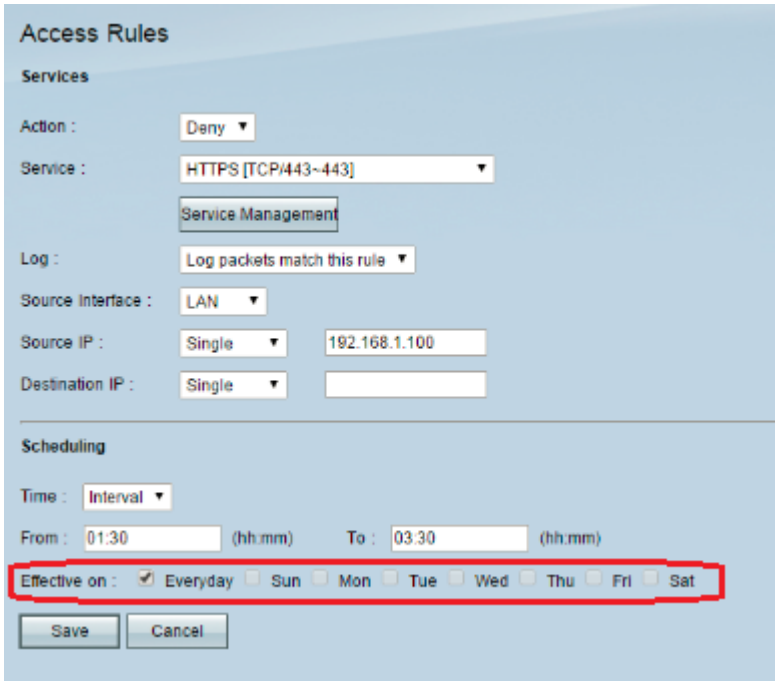
ãƒ» Immer â€" Diese Regel blockiert die Website ständig.

ãƒ» Intervall â€" Diese Regel blockiert die Website nur zu einer bestimmten Zeit oder an einem bestimmten Tag der Woche.

Schritt 12: Wenn Sie in Schritt 11 **Intervall** auswählen, geben Sie die gewünschte Start- und Endzeit in die Felder *Von* und *Bis ein*.



Schritt 13: Wenn Sie **Intervall** bei Schritt 11 auswählen, aktivieren Sie die gewünschten Tage, an denen Sie die Website blockieren möchten, oder aktivieren Sie das Kontrollkästchen **Täglich,** um die Website an jedem einzelnen Tag zu blockieren.



Schritt 14: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern. Die angegebene Website wird blockiert.

Wiederholen Sie Schritt 1 zu Schritt 15, um weitere URLs zu blockieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.