Web-Schutz für URL-Filterung auf RV016- und RV082-VPN-Routern

Ziel

Cisco ProtectLink Web ist eine Sicherheitsmaßnahme, die Spam, unerwünschte Inhalte und Spyware blockiert. Dies ist hilfreich, wenn Sie das Internet verwenden. Bevor Ihr Browser eine URL aufruft, überprüft Cisco ProtectLink Web die Website und blockiert alle Sicherheitsbedrohungen.

Eine Funktion von Cisco ProtectLink Web ist die Erstellung einer Liste mit genehmigten URLs. Der Webschutz für URL ist eine Funktion, die den Zugriff auf Websites anhand vordefinierter Kategorien blockiert. In diesem Artikel wird erläutert, wie Sie den Webschutz für URL auf RV082 VPN-Routern konfigurieren.

Unterstützte Geräte

RV082

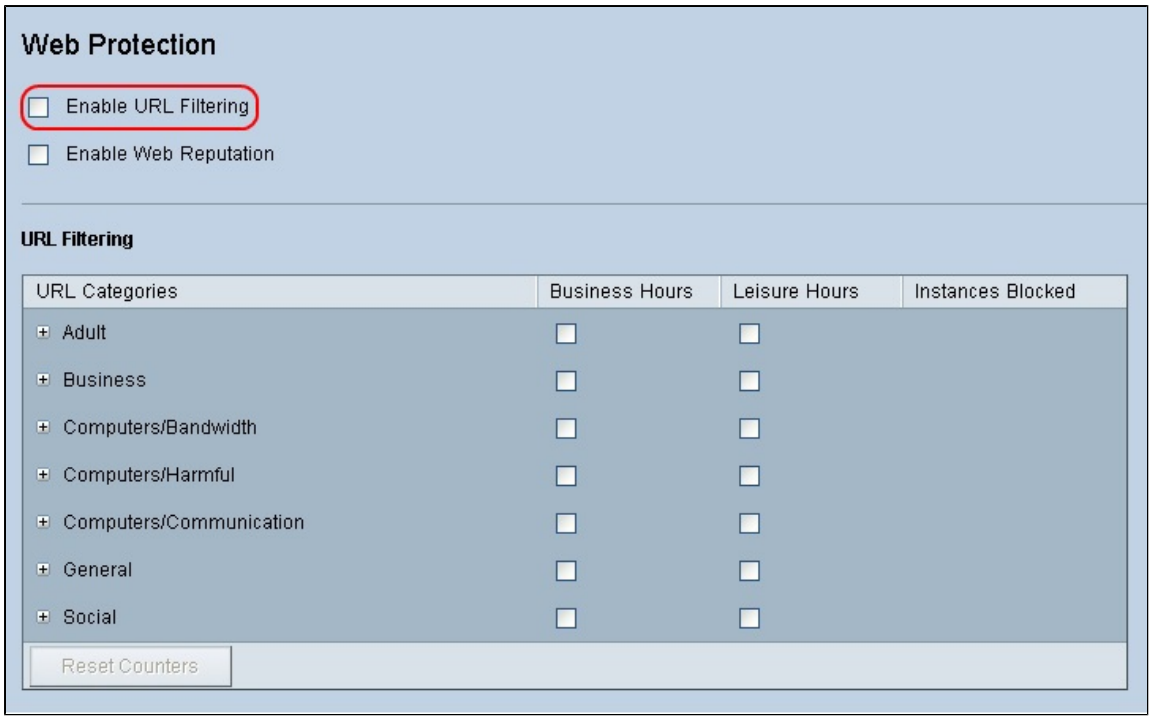
Software-Version

ã*f*» v4.2.2.08

URL-Filter

Hinweis: Stellen Sie vor Beginn der Konfiguration sicher, dass der ProtectLink-Zugriff auf dem Gerät aktiviert ist. Führen Sie die im Dokument *ProtectLink Web Registration and Activation* genannten Schritte *auf den RV082 VPN-Routern aus, um* ProtectLink zu aktivieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Cisco ProtectLink Web > Web Protection aus**. Die Seite *Webschutz* wird geöffnet:



Schritt 2: Aktivieren Sie das Kontrollkästchen **URL-Filterung aktivieren**, um die Filterung von URLs zu aktivieren.

Schritt 3: Aktivieren Sie das Kontrollkästchen **Geschäftszeiten** der Kategorien und Unterkategorien, die Sie während der Geschäftszeiten blockieren möchten. Um die Unterkategorien anzuzeigen, klicken Sie auf die Schaltfläche + neben einer Kategorie. Die Geschäftszeiten werden im Abschnitt *Geschäftsstundeneinstellungen* festgelegt.

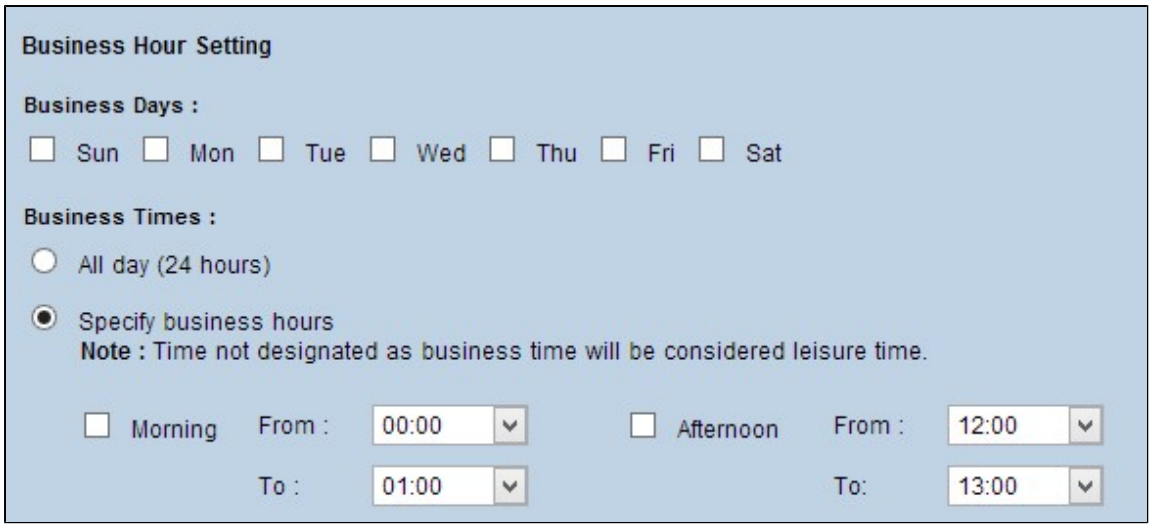
Schritt 4: Aktivieren Sie das Kontrollkästchen **Freizeit** für die Kategorien und Unterkategorien, die Sie während der Freizeit blockieren möchten. Als Freizeit gilt jede Zeit außerhalb der angegebenen Geschäftszeiten.

Schritt 5: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen rückgängig zu machen.

Geschäftsstundeneinstellungen

Scrollen Sie auf der *Web*-Schutzseite nach unten zum Abschnitt *Einstellung* der *Geschäftszeiten.* Hier können Sie bestimmen, welche Stunden als Geschäftszeiten gelten und welche Stunden als Freizeit gelten. Jede nicht berücksichtigte Geschäftszeit gilt als Freizeit.

Schritt 1: Wählen Sie im Feld *Geschäftstage* die Tage aus, auf die die URL-Filter für die Geschäftszeiten angewendet werden sollen.



Schritt 2: Klicken Sie im Feld *Geschäftszeiten* auf das Optionsfeld, das der Methode entspricht, mit der Sie die Geschäftszeiten bestimmen möchten. Folgende Optionen sind verfügbar:

ãƒ» Ganzer Tag (24 Stunden) â€" Filterung der Geschäftszeiten für den ganzen Tag.

ãƒ» Geschäftszeiten angeben â€" Legen Sie manuell den Zeitraum fest, für den die Geschäftsstundenfilterung angewendet werden soll.

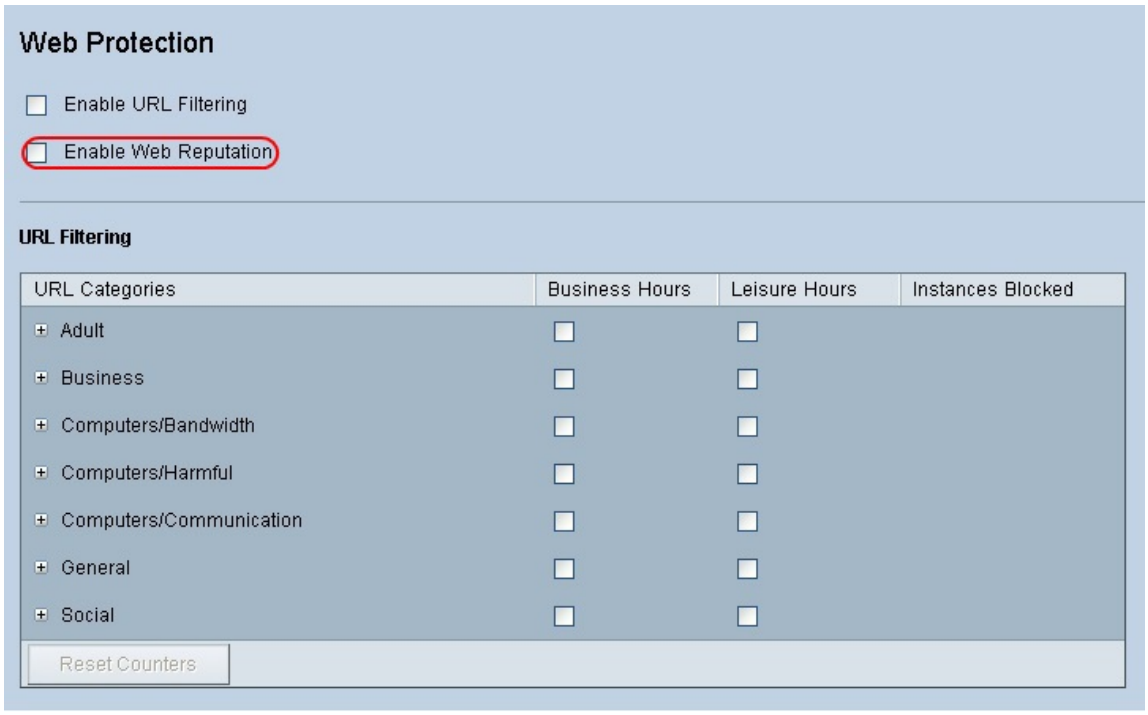
Schritt 3: Wenn Sie Geschäftszeiten angeben auswählen, aktivieren Sie das Kontrollkästchen **Morgen,** und wählen Sie aus den Dropdown-Listen Von und Bis aus, um die Geschäftszeiten am Morgen anzugeben. Aktivieren Sie das Kontrollkästchen **Nachmittag**, und wählen Sie aus den Dropdown-Listen die Zeiten Von und Bis aus, um die Geschäftszeiten am Nachmittag anzugeben.

Schritt 4: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen rückgängig zu machen.

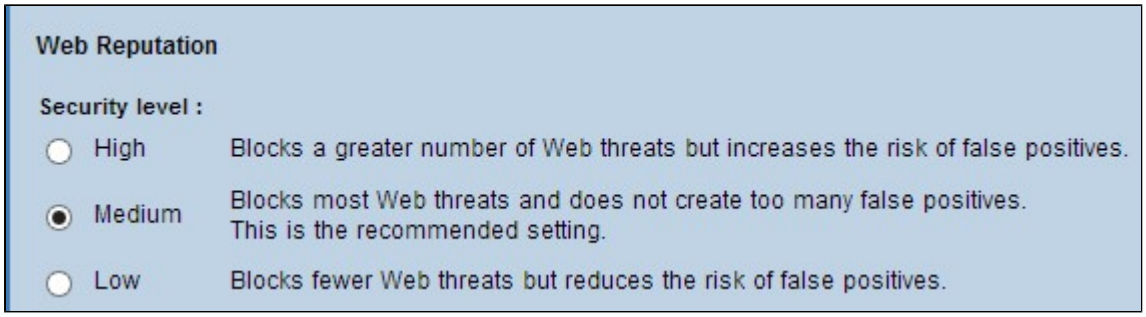
Webreputation

Webreputation hilft Ihnen, Bedrohungen für potenziell schädliche Websites zu verhindern. Es überprüft die Websites aus der Cisco ProtectLink Web Security-Datenbank.

Schritt 1: Aktivieren Sie das Kontrollkästchen **Webreputation aktivieren**, um die Webreputation zu aktivieren.



Schritt 2: Blättern Sie nach unten zum Feld *Webreputation*, und klicken Sie auf das Optionsfeld für die entsprechende Sicherheitsstufe.



ãƒ» Hoch - Diese Option blockiert eine größere Anzahl potenziell schädlicher Websites, hat aber auch eine höhere Inzidenz von Fehlalarmen (legitime Websites, die als schädlich klassifiziert werden).

ãƒ» Mittel: Diese Option blockiert die meisten potenziell schädlichen Websites und hat eine geringere Häufigkeit von Fehlalarmen. Die empfohlene Einstellung ist "Mittel".

ãƒ» Niedrig - Diese Option blockiert weniger potenziell schädliche Websites und reduziert somit das Risiko von Fehlalarmen.

Schritt 3: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen rückgängig zu machen.

URL-Überlaufsteuerung

Im Feld *URL Overflow Control* (URL-Überlaufsteuerung) können Sie festlegen, welche Aktion ausgeführt werden soll, wenn mehr URL-Anforderungen vorliegen, als der Dienst verarbeiten kann.

Schritt 1: Klicken Sie auf das Optionsfeld, das der Aktion entspricht, die ProtectLink im Falle eines Überlaufs ausführen soll. Folgende Optionen sind verfügbar:

ãƒ» URL-Anfragen vorübergehend blockieren â€" Dies ist eine empfohlene Standardeinstellung, die alle URL-Anfragen blockiert, bis die Anfragen verarbeitet werden.

ãƒ» Vorübergehende Umgehung der URL-Verifizierung für angeforderte URLs â€" Mit dieser Option können alle Anforderungen ohne Verifizierung weitergeleitet werden. Diese Einstellung wird nicht empfohlen.

Schritt 2: Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen rückgängig zu machen.

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.