Web bescherming voor URL-filtering inschakelen op RV016- en RV082 VPN-routers

Doel

Het Cisco ProtectLink-web is een beveiligingsmaatregel die spam, ongewenste inhoud en spyware blokkeert. Dit is handig als u internet gebruikt. Voordat uw browser een URL bezoekt, controleert Cisco ProtectLink Web de website en blokkeert alle bedreigingen voor de beveiliging.

Een van de functies van het Cisco ProtectLink-web is dat een gebruiker een lijst met goedgekeurde URLâ€™s kan maken. De webbeveiliging voor URL is een functie die helpt om toegang tot websites te blokkeren op basis van vooraf gedefinieerde categorieën. In dit artikel wordt uitgelegd hoe u de Web Protection for URL kunt configureren op RV082 VPN-routers.

Toepasselijke apparaten

· RV082

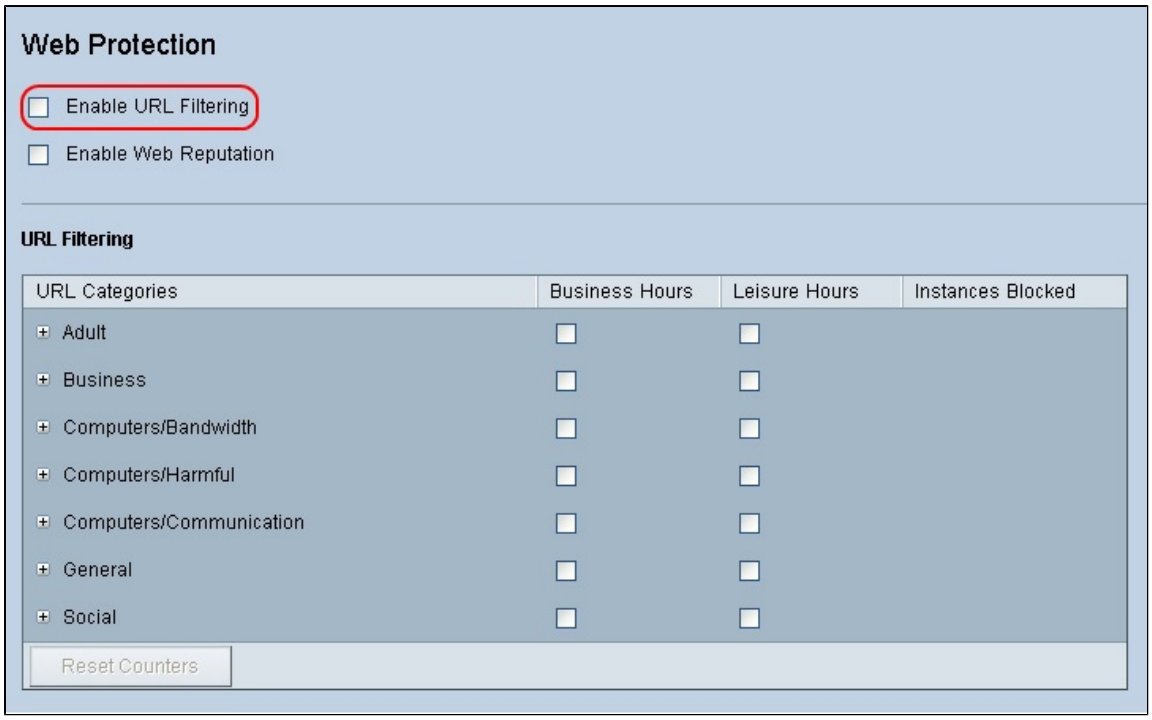
Softwareversie

· v4.2.2.08

URL-filter

Opmerking: voordat u begint met de configuratie moet u er zeker van zijn dat de ProtectLink-toegang is ingeschakeld in het apparaat. Volg de stappen die in het document *ProtectLink-webregistratie en -activering op de RV082 VPN-routers* worden vermeld om ProtectLink in te schakelen.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Cisco ProtectLink Web > Web Protection** (**Webbescherming)**. De pagina *Web Protection* wordt geopend:



Stap 2. Schakel het selectievakje **URL-filtering inschakelen in** om het filteren van URL's te activeren.

Stap 3. Vink het aanvinkvakje **Werkuren aan** voor de categorieën en subcategorieën die u tijdens kantooruren wilt blokkeren. Als u de subcategorieën wilt weergeven, klikt u op de knop + naast een categorie. De openingstijden worden ingesteld in het gedeelte *Instellingen kantooruren*.

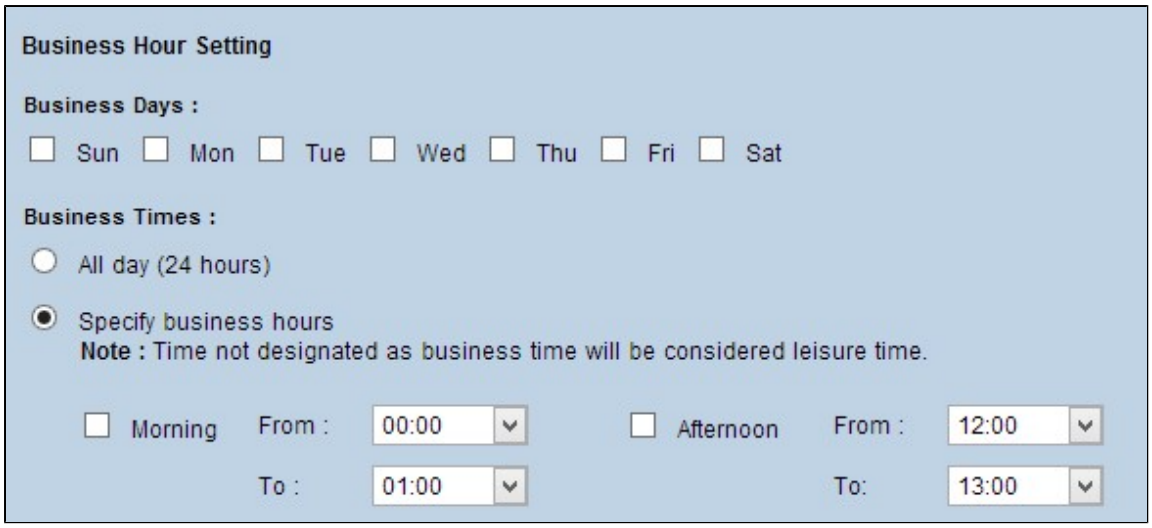
Stap 4. Vink het aanvinkvakje **Leisure Hours aan** van de categorieën en subcategorieën die u wilt blokkeren tijdens vrijetijdsuren. Vrijetijdsuren worden gedefinieerd als elk tijdstip buiten de opgegeven openingstijden.

Stap 5. Klik op **Opslaan** om wijzigingen op te slaan of op **Annuleren** om wijzigingen ongedaan te maken.

Instellingen kantooruren

Scroll naar het gedeelte *Business Hour Setting* op de pagina *Web Protection*, hier kunt u bepalen welke uren als kantooruren worden beschouwd en welke uren als vrijetijdsuren. Elk tijdstip dat niet als werktijd wordt beschouwd, wordt als vrijetijdsbesteding beschouwd.

Stap 1. Kies in het veld *Werkdagen* de dagen waarop u de URL-filters voor het kantooruur wilt toepassen.



Stap 2. Klik in het veld *Business Times* op het keuzerondje dat overeenkomt met de methode die u wilt gebruiken om de openingstijden te bepalen. De beschikbare opties zijn:

· De hele dag (24 uur) â€" Pas het werkuurfilter toe voor de hele dag.

· Specificeer kantooruren â€" Stel handmatig de tijdsperiode in waarvoor de werkuurfiltering geldt.

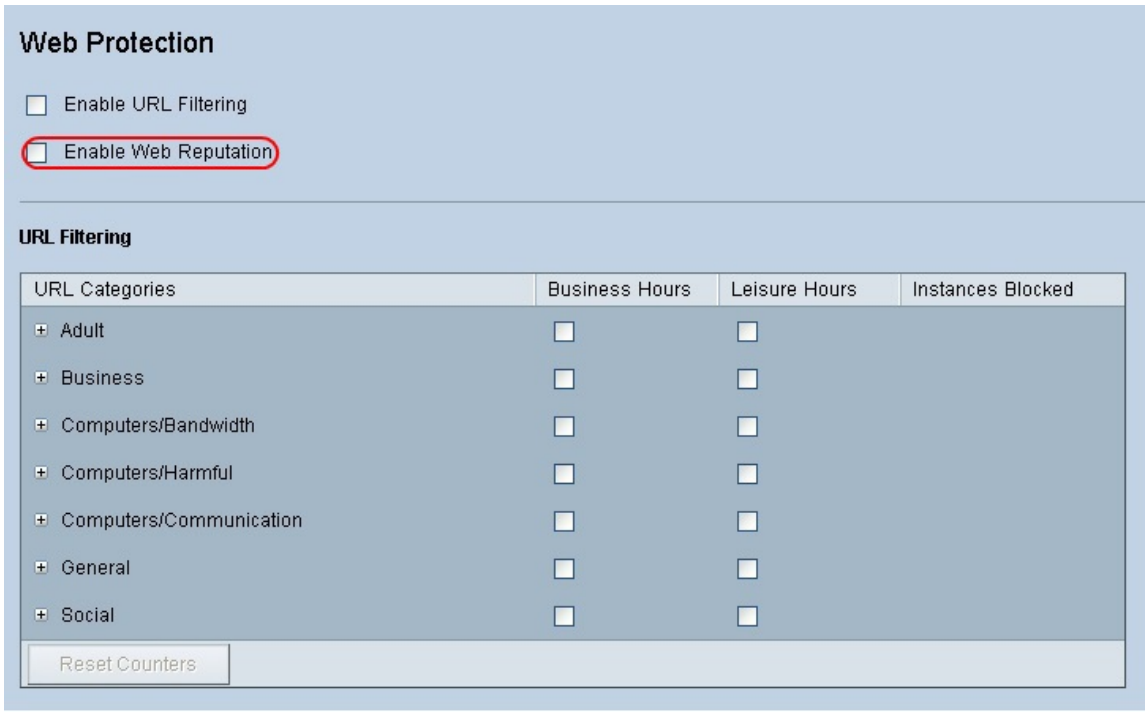
Stap 3. Als u Werkuren specificeren kiest, schakelt u het aanvinkvakje **'s ochtends in** en kiest u uit de vervolgkeuzelijsten Van en Tot tijden om de werktijden 's morgens aan te geven. Vink het aanvinkvakje **middag** aan en kies de Van en Tot tijden uit de vervolgkeuzelijsten om de kantooruren in de middag te specificeren.

Stap 4. Klik op **Opslaan** om wijzigingen op te slaan of op **Annuleren** om wijzigingen ongedaan te maken.

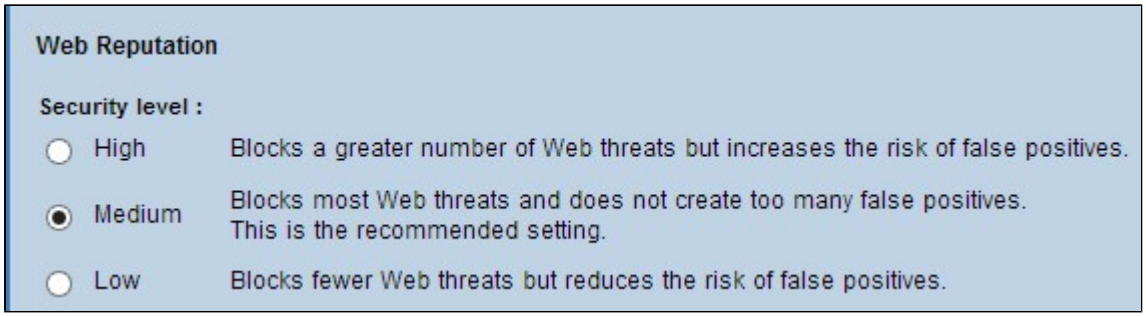
Webreputatie

Web Reputation helpt u om bedreigingen tegen potentieel schadelijke websites te voorkomen. Het verifieert de websites van het gegevensbestand van de Veiligheid van het Web van Cisco ProtectLink.

Stap 1. Schakel het aanvinkvakje **Enable Web Reputation in** om Web Reputation in te schakelen.



Stap 2. Blader naar beneden naar het veld *Webreputatie* en klik op het keuzerondje van het juiste beveiligingsniveau.



· Hoog - Deze optie blokkeert een hoger aantal potentieel kwaadaardige websites, maar heeft ook een hogere incidentie van vals positieven (legitieme sites die worden geclassificeerd als kwaadaardig).

· Medium - Deze optie blokkeert de meest potentieel schadelijke websites, en heeft een lagere incidentie van vals positieven. Gemiddeld is de aanbevolen instelling.

· Laag - Deze optie blokkeert minder potentieel kwaadaardige websites, en vermindert daarom het risico van valse positieven.

Stap 3. Klik op **Opslaan** om wijzigingen op te slaan of op **Annuleren** om wijzigingen ongedaan te maken.

URL-overloopcontrole

In het veld *URL Overflow Control* kunt u bepalen welke actie moet worden ondernomen als er meer URL-aanvragen zijn dan de service kan verwerken.

Stap 1. Klik op het keuzerondje dat overeenkomt met de actie die u wilt dat ProtectLink in het geval van een overloop neemt. De beschikbare opties zijn:

· Blokkeer tijdelijk URL-verzoeken â€” Dit is een aanbevolen en standaardinstelling die alle URL-verzoeken blokkeert totdat de verzoeken worden verwerkt.

· Tijdelijk de URL-verificatie voor aangevraagde URLâ€™s omzeilen â€” Met deze optie kunnen alle aanvragen zonder verificatie worden doorgegeven. Deze instelling wordt niet aanbevolen.

Stap 2. Klik op **Opslaan** om wijzigingen op te slaan of op **Annuleren** om wijzigingen ongedaan te maken.

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.