

Configurazione di Content Filtering su RV160 e RV260

Obiettivo

L'obiettivo di questo articolo è mostrare come configurare e gestire le impostazioni di filtro dei contenuti sui router RV160 e RV260.

Introduzione

La funzionalità di filtro dei contenuti consente di limitare l'accesso a determinati siti Web indesiderati. Può bloccare l'accesso ai siti Web in base ai nomi di dominio e alle parole chiave. È inoltre possibile pianificare quando il filtro contenuti è attivo. Il filtro dei contenuti può migliorare una rete già sicura e promuovere la produttività sul posto di lavoro bloccando o autorizzando i siti Web in determinati momenti.

Questa funzionalità inclusa è applicabile solo ai siti **http://**. Questo significa che i siti attendibili che iniziano con **https://**, inclusi Facebook e YouTube, non possono essere bloccati. [Per ulteriori informazioni sulle opzioni di gestione dell'accesso agli URL, fare clic qui.](#)

Dispositivi interessati

- RV160
- RV260

Versione del software

- 1.0.00.15

Configura Content Filtering

Per configurare e abilitare il filtro contenuti su RV160/RV260, attenersi alla seguente procedura.

Passaggio 1. Accedere alla pagina di configurazione Web del router.



Router

cisco 1

..... 2

English ▼

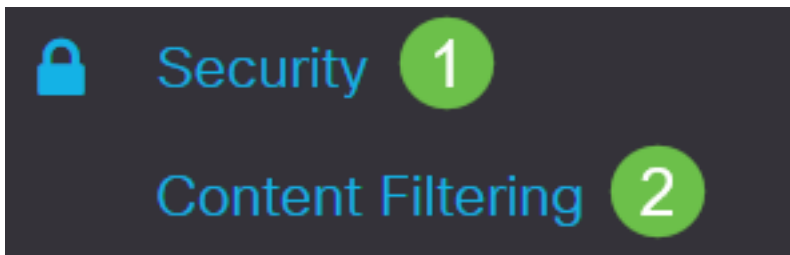
Login 3

©2018 Cisco Systems, Inc. All Rights Reserved.

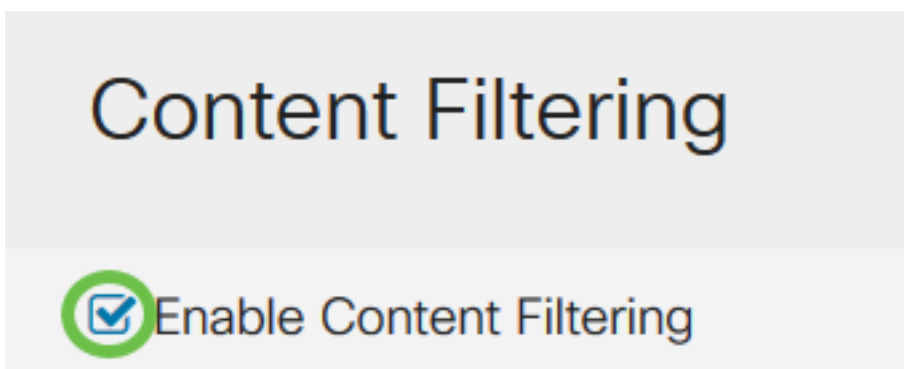
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

In questo articolo, utilizzeremo la RV160 per configurare il filtro dei contenuti. La configurazione può variare a seconda del modello in uso.

Passaggio 2. Passare a **Sicurezza > Content Filtering**.



Passaggio 3. Selezionare *Abilita filtro contenuto* per abilitarlo.



Passaggio 4. Selezionare una delle opzioni seguenti:

- Blocca URL corrispondenti - Selezionare *Blocca URL corrispondenti* per bloccare domini e parole chiave specifici
- Consenti solo URL corrispondenti: selezionare *Consenti solo URL corrispondenti* per consentire solo i domini e le parole chiave specificati

Nell'esempio è selezionata l'opzione **Blocca URL corrispondenti**.

Content Filtering

Enable Content Filtering

Block Matching URLs

Allow Only Matching URLs

Passaggio 5. In *Filtra per dominio*, fare clic su **Aggiungi**.

Content Filtering

Enable Content Filtering

Block Matching URLs

Allow Only Matching URLs

Filter by Domain



Domain Name

Schedule

Passaggio 6. Immettere il dominio da filtrare o consentire nella colonna *Nome dominio*.

Nell'esempio, il nome del dominio specificato è *www.internetbadguys.com*.

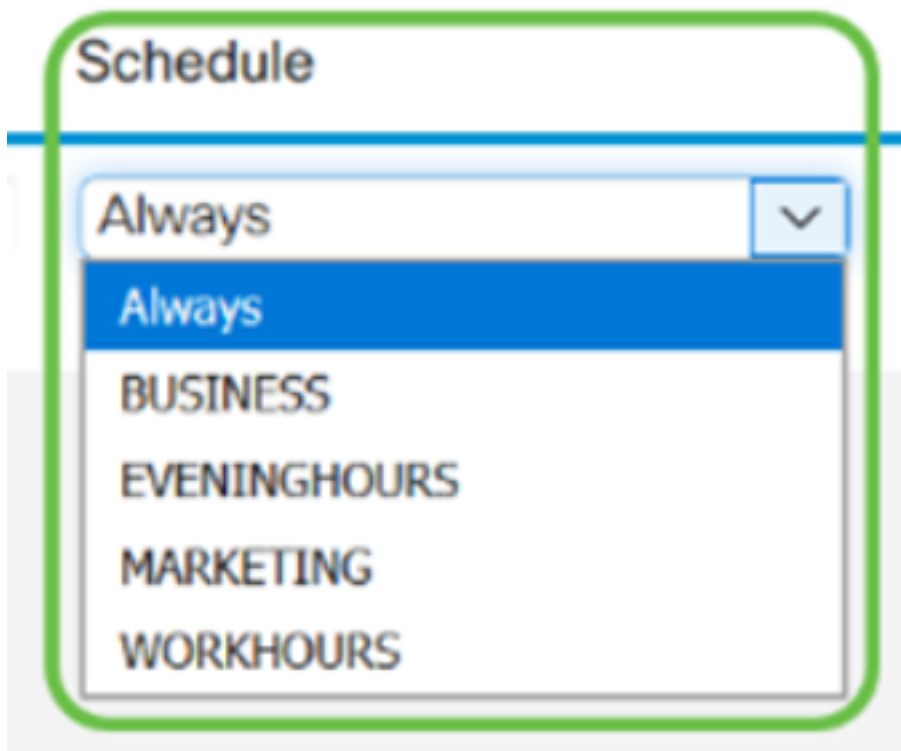
Filter by Domain



Domain Name

Passaggio 7. Per specificare quando le regole di filtro del contenuto sono attive, selezionare la pianificazione dall'elenco a discesa *Pianificazione*.

In questo esempio, la pianificazione scelta è **Sempre**.



Passaggio 8. In *Filtra per parola chiave*, fare clic su **Add**.

Filter by Keyword



Keyword

internetbadguys

Passaggio 9. Immettere le parole chiave da bloccare o consentire nella colonna *Nome parola chiave*.

Nell'esempio, la parola chiave viene immessa come Facebook.

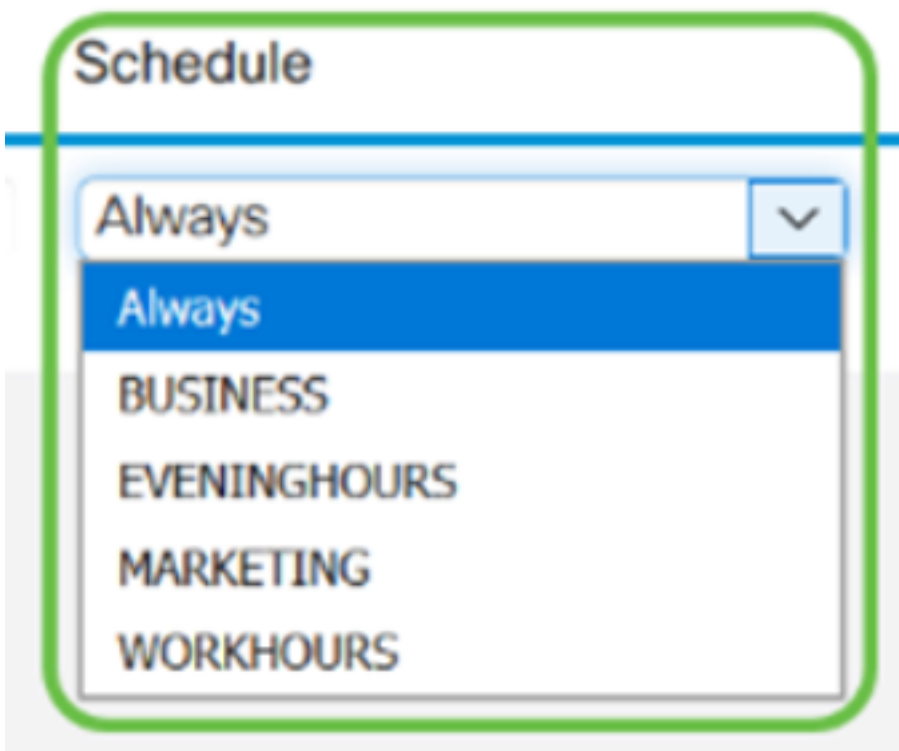
Filter by Keyword



Keyword

internetbadguys

Passaggio 10. Per specificare quando le regole di filtro del contenuto sono attive, selezionare la pianificazione dall'elenco a discesa *Pianificazione*.



Passaggio 11. È possibile modificare un nome di *dominio* o di *parola chiave* esistente selezionando il nome e facendo clic su **Modifica**.

Content Filtering

- Enable Content Filtering
- Block Matching URLs
- Allow Only Matching URLs

Filter by Domain



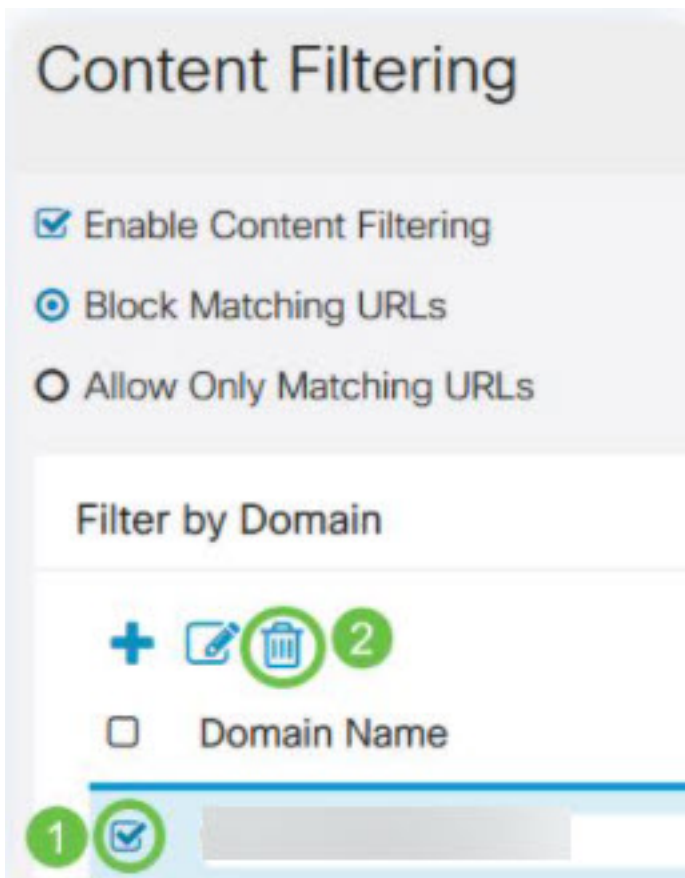
Domain Name

1

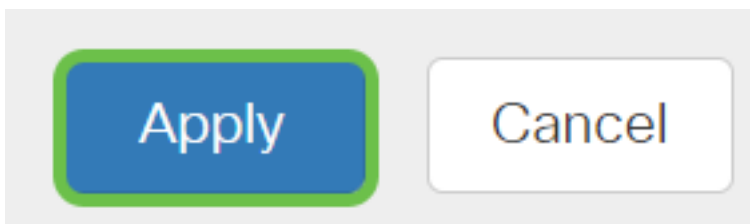


[Redacted text]

Passaggio 12. È possibile eliminare un nome di *dominio* o di *parola chiave* esistente selezionando il nome e facendo clic su **Elimina**.



Passaggio 13. Fare clic su **Applica**.



A questo punto, è necessario aver abilitato e configurato correttamente il filtro contenuti sul router RV160/ RV260.

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)