RV016 및 RV082 VPN 라우터에서 URL 필터링을 위한 웹 보호 활성화

목표

Cisco ProtectLink 웹은 스팸, 원치 않는 콘텐츠 및 스파이웨어를 차단하는 보안 조치입니다.이는 인터넷을 사용할 때 유용합니다.브라우저에서 URL을 방문하기 전에 Cisco ProtectLink Web에서 웹 사이트를 확인하고 보안에 대한 모든 위협을 차단합니다.

Cisco ProtectLink Web의 한 가지 기능은 사용자가 승인된 URL 목록을 생성할 수 있다는 것입니다.URL에 대한 웹 보호는 미리 정의된 카테고리를 기반으로 웹 사이트에 대한 액세스를 차단하는 데 도움이 되는 기능입니다.이 문서에서는 RV082 VPN 라우터의 URL에 대한 웹 보호를 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

·RV082

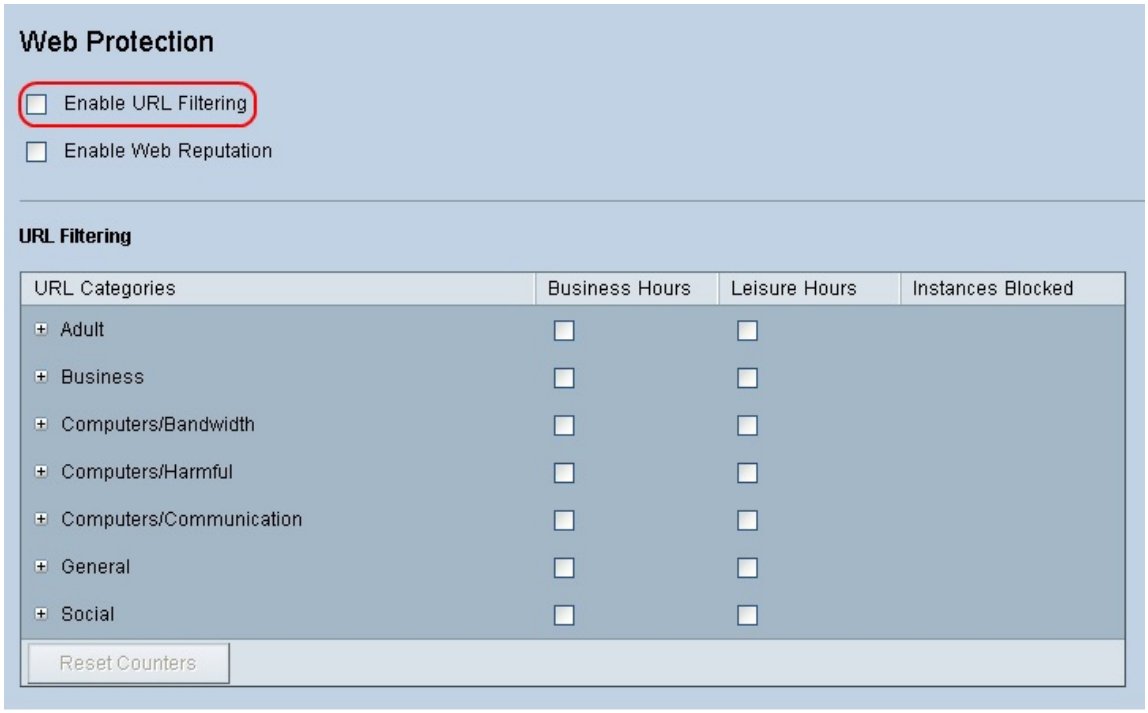
소프트웨어 버전

·v4.2.2.08

URL 필터

참고:컨피그레이션을 시작하기 전에 디바이스에서 ProtectLink 액세스가 활성화되어 있는지 확인하십시오.ProtectLink를 활성화하려면 RV*082 VPN 라우터에서 ProtectLink Web Registration and Activation(ProtectLink 웹 등록 및 활성화)* 문서에 설명된 단계를 수행합니다.

1단계. 웹 구성 유틸리티에 로그인하고 **Cisco ProtectLink Web > Web Protection을** 선택합니다.*웹 보호* 페이지가 열립니다.



2단계. Enable **URL Filtering(URL 필터링 활성화)** 확인란을 선택하여 URL 필터링을 활성화합니다.

3단계. 업무 시간 중에 차단하려는 범주 및 하위 범주의 **업무 시간** 체크박스를 선택합니다.하위 범주를 보려면 범주 옆에 있는 **+**버튼을 클릭합니다.업무 시간은 업무 시간 *설정* 섹션에서 설정됩니다.

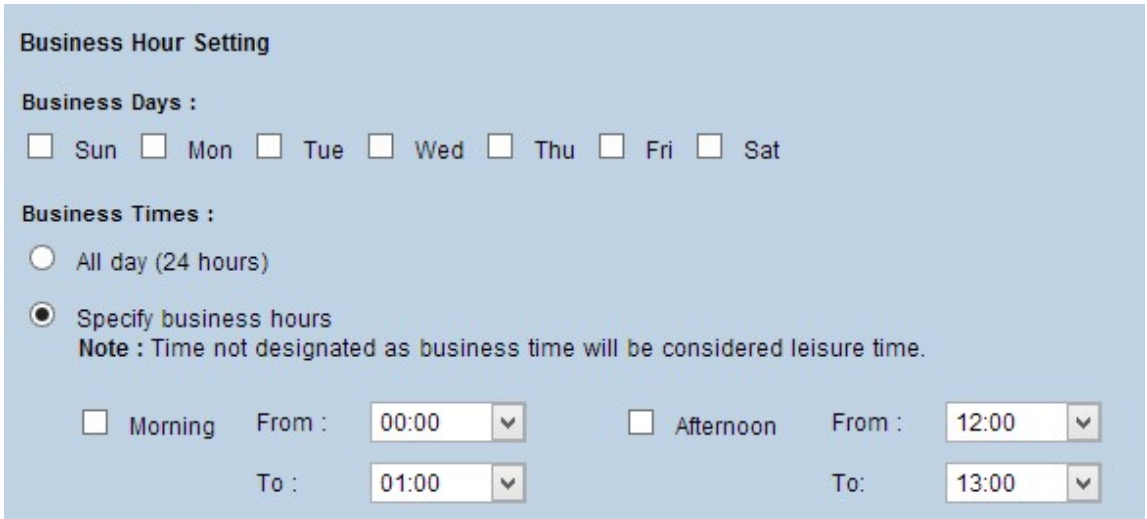
4단계. **여가** 시간 동안 차단할 범주 및 하위 범주의 **Leisure Hours** 확인란을 선택합니다.여가 시간은 지정된 업무 시간 이외의 시간으로 정의됩니다.

5단계. **저장**을 클릭하여 변경 사항을 저장하거나 **취소**를 클릭하여 변경 사항을 취소합니다.

업무 시간 설정

웹 보호 페이지의 *업무 시간 설정* 섹션으로 스크롤하여 업무 시간으로 간주되는 시간과 여가 시간으로 간주되는 시간을 결정할 수 있습니다.업무 시간으로 간주되지 않는 모든 시간은 여가 시간으로 간주될 것이다.

1단계. *Business Days* 필드에서 업무 시간 URL 필터를 적용할 날짜를 선택합니다.



2단계. *Business Times* 필드에서 업무 시간을 결정하는 데 사용할 방법에 해당하는 라디오 버튼을 클릭합니다.사용 가능한 옵션은 다음과 같습니다.

·하루 종일(24시간) — 하루 종일 업무 시간 필터링을 적용합니다.

·업무 시간 지정 — 업무 시간 필터링이 적용되는 기간을 수동으로 설정합니다.

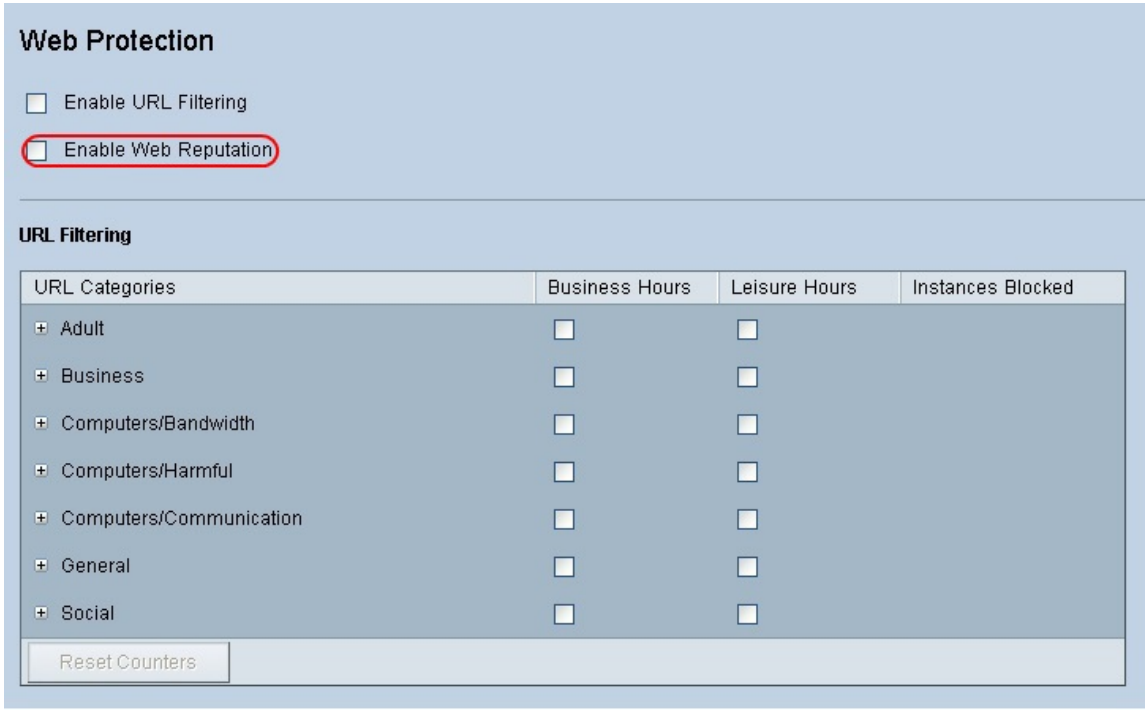
3단계. 업무 시간 지정을 선택한 경우 **오전** 체크박스를 선택하고 드롭다운 목록에서 시작 및 종료 시간을 선택하여 오전 업무 시간을 지정합니다.**Afternoon** 확인란을 선택하고 드롭다운 목록에서 From 및 To 시간을 선택하여 오후 업무 시간을 지정합니다.

4단계. **저장**을 클릭하여 변경 사항을 저장하거나 **취소**를 클릭하여 변경 사항을 취소합니다.

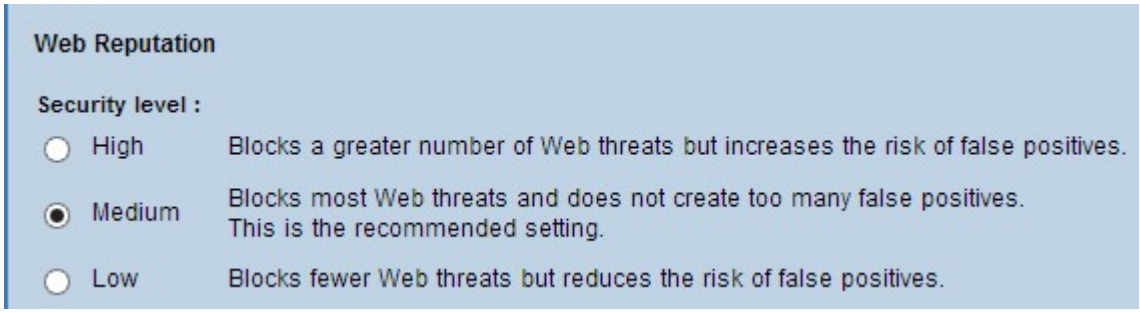
웹 평판

웹 평판은 악성 웹 사이트에 대한 위협을 방지하는 데 도움이 됩니다.Cisco ProtectLink Web Security 데이터베이스에서 웹 사이트를 확인합니다.

1단계. Enable **Web Reputation(웹 평판 활성화)** 확인란을 선택하여 웹 평판을 활성화합니다.



2단계. 아래로 스크롤하여 *Web Reputation(웹 평판)* 필드로 이동하고 적절한 보안 레벨의 라디오 버튼을 클릭합니다.



·높음 - 이 옵션은 악의적인 웹 사이트의 수를 차단하지만 오탐(악성으로 분류된 합법적인 사이트)의 발생률이 높습니다.

·Medium(중간) - 이 옵션은 대부분의 악성 웹 사이트를 차단하며 오탐 발생률이 낮습니다.권장 설정입니다.

·낮음 - 이 옵션은 잠재적으로 악의적일 가능성이 있는 웹 사이트를 더 적게 차단하여 오탐의 위험을 줄입니다.

3단계. **저장**을 클릭하여 변경 사항을 저장하거나 **취소**를 클릭하여 변경 사항을 취소합니다.

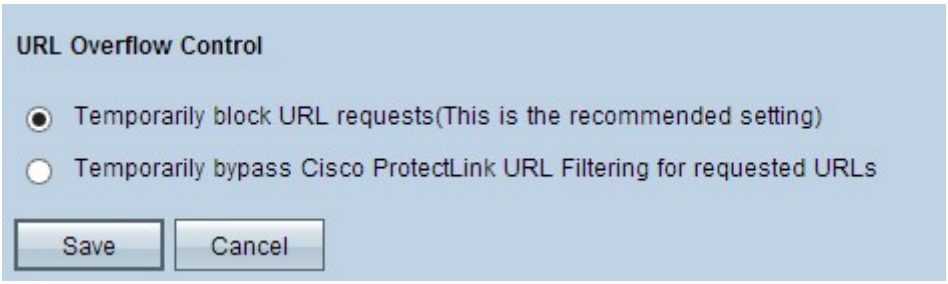
URL 오버플로 제어

URL Overflow *Control(URL 오버플로 제어*) 필드에서 서비스가 처리할 수 있는 것보다 더 많은 URL 요청이 있을 때 수행할 작업을 결정할 수 있습니다.

1단계. 오버플로가 발생할 경우 ProtectLink에서 수행할 작업에 해당하는 라디오 버튼을 클릭합니다.사용 가능한 옵션은 다음과 같습니다.

·일시적으로 URL 요청 차단 — 요청을 처리할 때까지 모든 URL 요청을 차단하는 권장 및 기본 설정입니다.

·요청된 URL에 대한 URL 확인을 일시적으로 우회 — 이 옵션을 사용하면 모든 요청을 확인 없이 전달할 수 있습니다.이 설정은 권장되지 않습니다.



2단계. **저장**을 클릭하여 변경 사항을 저장하거나 **취소**를 클릭하여 변경 사항을 취소합니다.