

RV320和RV325路由器上的基本防火墙配置

目标

本文介绍如何在RV32x VPN路由器系列上配置基本防火墙设置。

防火墙是一组旨在保护网络安全的功能。路由器被视为强大的硬件防火墙。这是因为路由器能够检查所有入站流量并丢弃任何不需要的数据包。网络防火墙可保护内部计算机网络（家庭、学校、企业内部网）免受外部恶意访问。还可以配置网络防火墙以限制内部用户对外部的访问。

适用设备

- RV320双WAN VPN路由器
- RV325千兆双WAN VPN路由器

软件版本

- v1.1.0.09

基本设置

步骤1. 登录Web配置实用程序，然后选择“防火墙”>“常规”。将打开“一般信息”页：

General	
Firewall:	<input checked="" type="checkbox"/> Enable
SPI (Stateful Packet Inspection):	<input checked="" type="checkbox"/> Enable
DoS (Denial of Service):	<input checked="" type="checkbox"/> Enable
Block WAN Request:	<input checked="" type="checkbox"/> Enable
Remote Management:	<input checked="" type="checkbox"/> Enable Port: 443
Multicast Pass Through:	<input checked="" type="checkbox"/> Enable
HTTPS:	<input checked="" type="checkbox"/> Enable
SSL VPN:	<input checked="" type="checkbox"/> Enable
SIP ALG:	<input checked="" type="checkbox"/> Enable
UPnP:	<input type="checkbox"/> Enable
<hr/>	
Restrict Web Features	
Block:	<input type="checkbox"/> Java <input checked="" type="checkbox"/> Cookies <input checked="" type="checkbox"/> ActiveX <input checked="" type="checkbox"/> Access to HTTP Proxy Servers
Exception:	<input checked="" type="checkbox"/> Enable

步骤2.根据您的要求，选中与要启用的功能对应的**Enable**复选框。

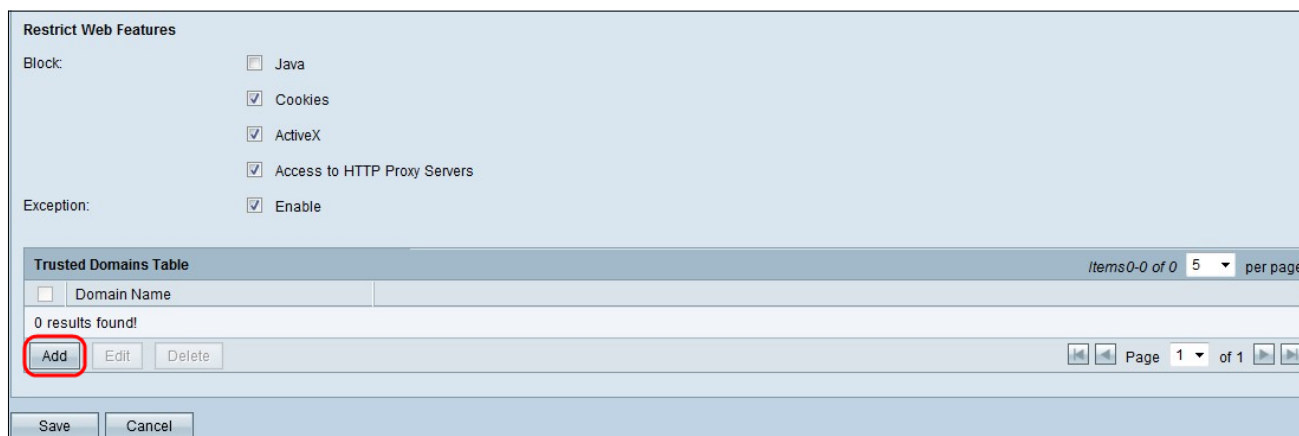
- 防火墙 — 路由器防火墙可以关闭（禁用），也可以启用它们以通过所谓的防火墙规则过滤某些类型的网络流量，防火墙可用于过滤所有传入和传出流量并基于这些流量。
- SPI（状态数据包检测） — 监控网络连接的状态（如TCP流和UDP通信）防火墙区分不同类型的连接的合法数据包。防火墙仅允许与已知活动连接匹配的数据包，其他所有数据包均被拒绝。
- DoS（拒绝服务） — 用于保护网络免受分布式拒绝服务(DDoS)攻击。DDoS攻击旨在将网络泛洪到网络资源不可用的位置。RV320使用DoS保护通过限制和删除不需要的数据包来保护网络。
- 阻止WAN请求 — 阻止从WAN端口向路由器发出的所有ping请求。
- 远程管理 — 允许从远程WAN网络访问路由器。
 - 端口 — 输入要远程管理的端口号。
- Multicast Pass Through — 允许IP组播消息通过设备。
- HTTPS（安全超文本传输协议） — 用于通过计算机网络进行安全通信的通信协议。它从客户端和服务端提供双向加密。
- SSL VPN — 允许通过路由器建立SSL VPN连接。
- SIP ALG - SIP ALG提供的功能允许在使用网络地址和端口转换(NAPT)时从防火墙的私有到公共和公共到私有端的IP语音流量。NAPT是最常见的网络地址转换类型。
- UPnP（通用即插即用） — 允许自动发现可与路由器通信的设备。

步骤3.根据您的要求，选中与要阻止的功能对应的**Enable**复选框。

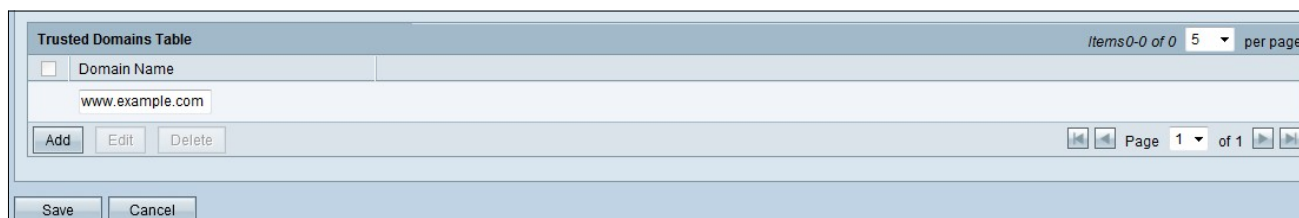
- Java — 选中此框将阻止下载和执行Java小程序。Java是许多网站使用的一种通用编程语言。但是，为恶意目的而制作的Java小程序可能会对网络造成安全威胁。下载后，恶意java小程序可以利用网络资源。
- Cookie — 网站创建Cookie以存储有关用户的信息。Cookie可以跟踪用户的Web历史记录，这可能导致隐私受到侵犯。
- ActiveX - ActiveX是许多网站使用的小程序类型。虽然通常是安全的，但一旦在计算机上安装了恶意的ActiveX小程序，用户可以执行任何操作。它可能会将有害代码插入操作系统、浏览安全内联网、更改密码或检索和发送文档。
- 对HTTP代理服务器的访问 — 代理服务器是提供两个独立网络之间链路的服务器。恶意代理服务器可以记录发送到它们的任何未加密数据，例如登录或密码。
- 异常 — 允许所选功能（Java、Cookie、ActiveX或HTTP代理服务器访问），但限制配置的受信任域上所有未选功能。受信任并有权访问受信任网络的域。您可以设置一个可信域，允许外部域的用户访问您的网络资源。如果禁用此选项，则受信任域允许所有功能。

注意：节省时间：如果您尚未选中Exception复选框，则跳过第4步。

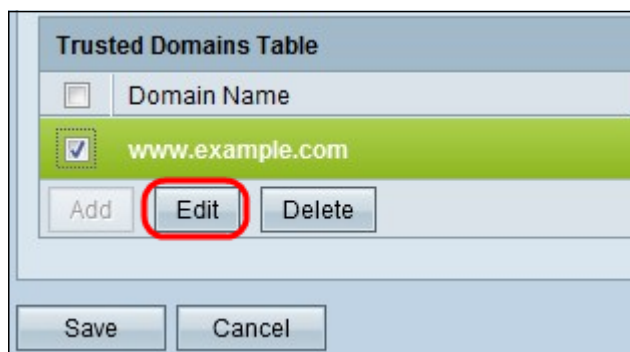
步骤4.点击Add，输入新的受信任域，然后点击Save以创建受信任域。



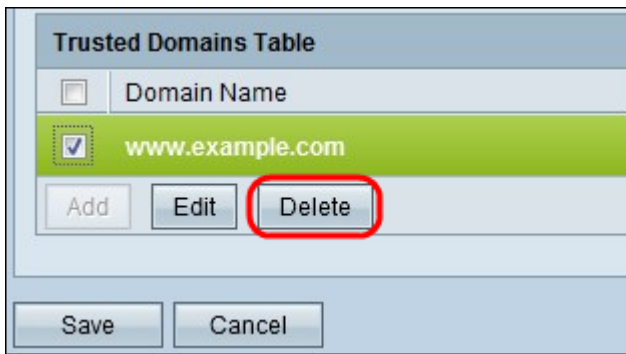
步骤5.点击Save更新更改。



第6步。（可选）要编辑受信任域的名称，请选中要编辑的受信任域的复选框，点击编辑，编辑域名，然后点击保存。



步骤7。（可选）要删除受信任域列表中的域，请选中要删除的受信任域的复选框，然后点击删除。



[查看与本文相关的视频.....](#)

[单击此处查看思科提供的其他技术讲座](#)