在CVR100W VPN路由器的基本的防火墙配置

客观

防火墙是设计的功能集合保持网络安全。路由器认为一严格的硬件防火墙。这归结于事实路由器能检查所有Inbound数据流和丢弃所有不需要的信息包。此条款说明如何配置在CVR100W VPN路由器的基本的防火墙设置。

可适用的设备

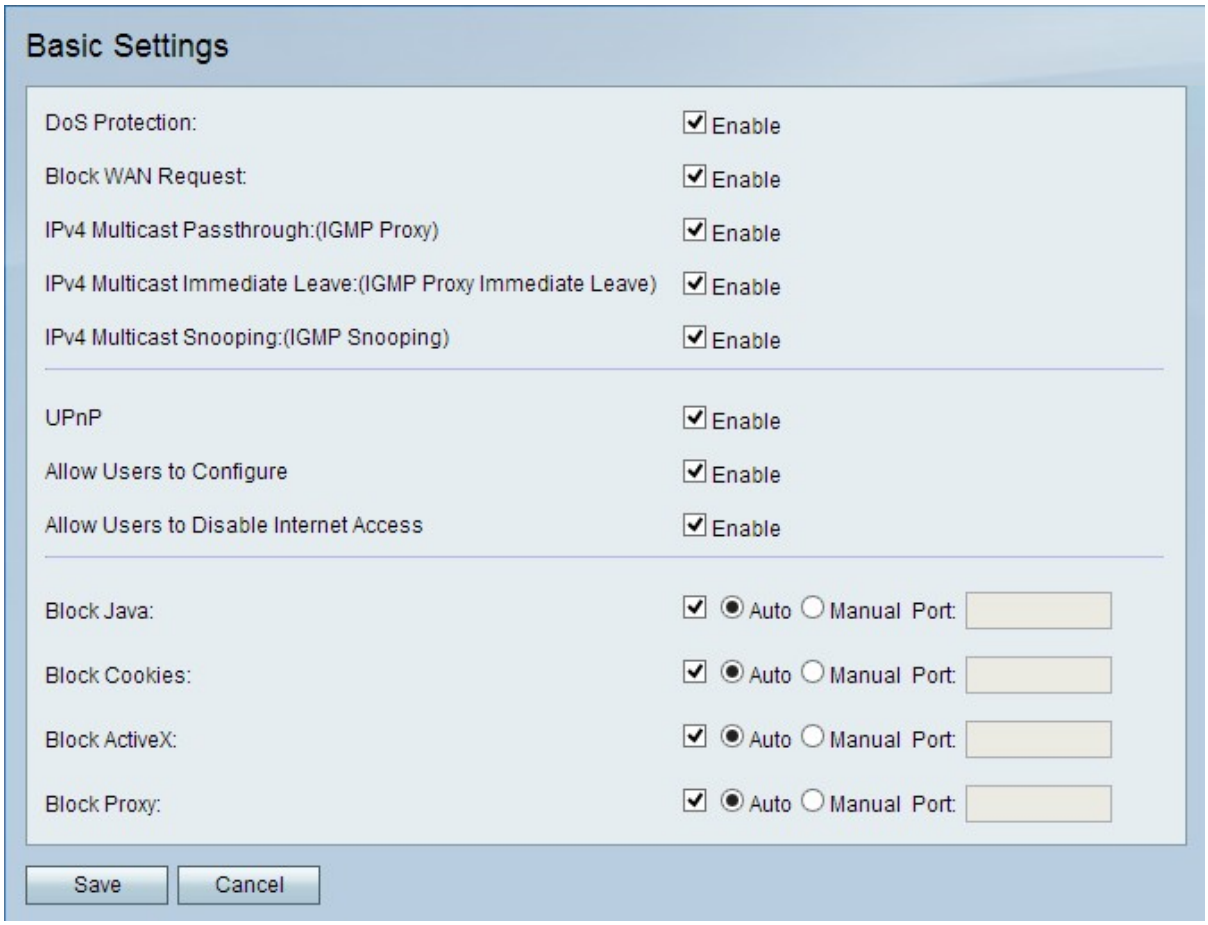
•CVR100W

软件版本

•1.0.1.19

基本的防火墙配置

步骤1.登陆到Web配置工具并且选择**防火墙>基本设置**。*基本设置*页打开：



Note:第2步到第13步是可选的。您能配置根据您的需要的这些选项。

步骤2.为了enable (event)在CVR100W的拒绝服务保护，检查在DoS保护字段的**Enable (event)**。DoS保护用于防止网络分布式拒绝服务(DDos)攻击。DDoS攻击被认为充斥网络到网络资源变得未提供的点。CVR100W使用DoS保护通过不需要的信息包限制和删除保护网络。

步骤3.为了拒绝所有ping请求到从广域网的CVR100W，请检查在块广域网请求字段的**Enable (event)**。

步骤4.为了允许IPv4组播数据流通过CVR100W来自互联网，请检查在IPv4组播转接字段的**Enable (event)**。IP组播是使用发送IP数据包到一个选定的组在单个发射的接受器的方法。

步骤5. IGMP代理是路由器的一个方式能与其它设备呼应使用IGMP消息传送。立即事假enable (event)离开组播组的CVR100W以最佳的速度。对enable (event) IGMP代理立即事假，请检查在IPv4组播立即事假字段的**Enable (event)**。

步骤6.为了允许在网络的其他交换机监听到反复去在计算机和CVR100W之间的消息监听的enable (event) IGMP，检查在IPv4组播监听的字段的**Enable (event)**。

步骤7.为了enable (event)通用即插即用(UPnP)，检查在UPnP字段的**Enable (event)**。UPnP允许能与CVR100W联络在设备的自动发现上。

步骤8.为了允许用户用UPnP能够设备配置UPnP端口映射规则，在允许用户的检查**Enable (event)**到Configure字段。端口映射或端口转发用于允许外部在专用LAN内提供的主机和服务之间的通信。

步骤9.为了允许用户禁用对设备的互联网访问，在允许用户的检查**Enable (event)**禁用互联网访问字段。

步骤10.为了阻拦从下载的Java程序，请检查在块Java字段的**块Java**。为恶意目的做的Java程序能造成对网络的一个安全威胁。一旦下载，敌对Java程序能利用网络资源。点击对应于期望块方法的单选按钮。

- 自动—自动地阻拦Java。
- 手工的端口—输入阻拦Java的一个特定端口。

第11.步。如果不希望网站创建Cookie，请检查在块Cookie领域的**块Cookie**。Cookie是由网站创建的存储这些用户的信息。Cookie能跟踪可能导致秘密侵入用户的Web历史记录。点击对应于期望块方法的单选按钮。

- 自动—自动块Cookie。
- 手工的端口—输入阻拦Cookie的一个特定端口。

步骤12。为了阻拦从下载的ActiveX附属程序，请检查在块ActiveX字段的**块ActiveX**。ActiveX是缺乏安全附属程序的类型。一旦ActiveX附属程序在计算机上安装，能执行用户能执行的任何东西。它可能插入有害的代码到操作系统，冲浪一个安全的内部网，更改密码或者检索和寄发文件。点击对应于期望块方法的单选按钮。

- 自动—自动块ActiveX。
- 手工的端口—输入阻拦ActiveX的一个特定端口。

第13步。为了阻拦代理服务器，请检查在块代理字段的**块代理**。代理服务器是提供两个独立的网络之间的一条链路的服务器。有恶意的代理服务器能记录被发送到他们例如登录或密码的所有未加密的数据。点击对应于期望块方法的单选按钮。

- 自动—自动块代理服务器。
- 手工的端口—输入阻拦代理服务器的一个特定端口。

步骤14。点击“Save”保存您做的所有变动。