# WRVS4400N无线N千兆位安全路由器的入侵防御系统(IPS)配置

## 客观

入侵防御系统(IPS)是该网络安全设备的恶意活动的监控网络活动。IPS的主要功能将识别，产生信息关于，块和报告恶意活动用户。

此条款目标将解释如何配置IPS和了解关于WRVS4400N无线N千兆位安全路由器的信息报告。

## 可适用的设备

•WRVS4400N

## 软件版本

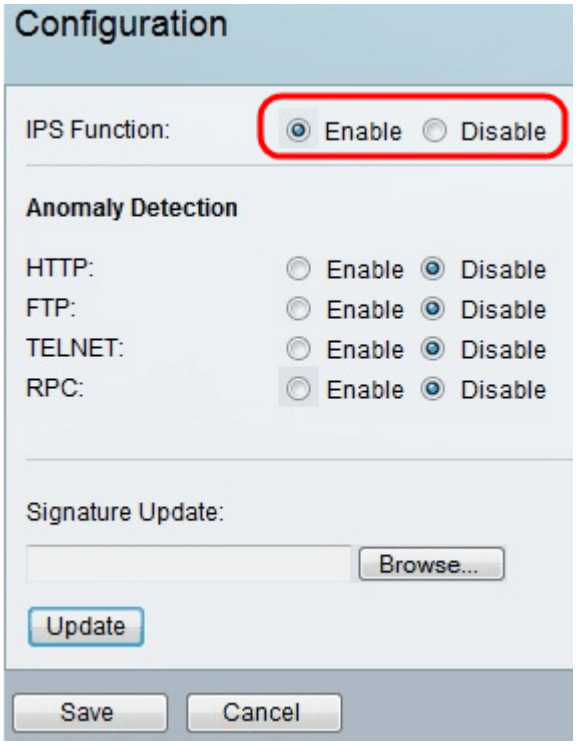
•v2.0.2.1

## 入侵防御系统

### 入侵防御系统配置

步骤1.登陆在Web配置工具并且选择**IPS >配置**，并且*IPS*配置页打开：


步骤2.点击**Enable单选按钮**对enable (event)路由器的IPS功能。



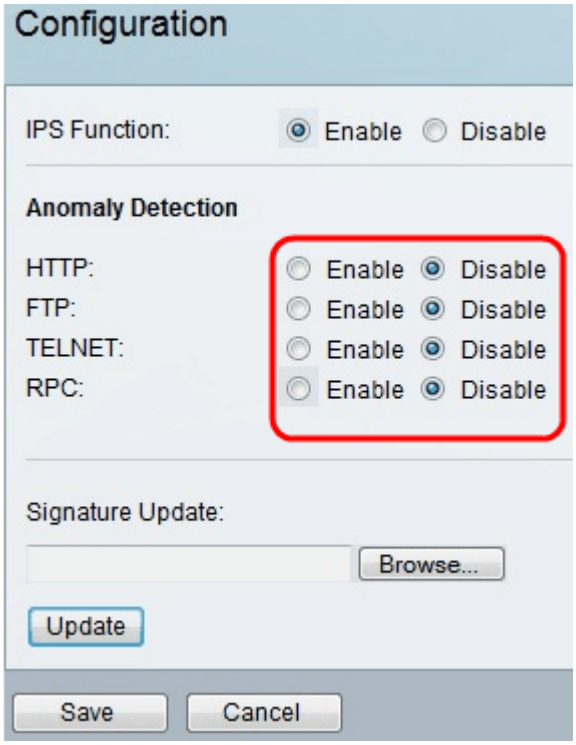

步骤3.点击**Enable (event)**或**禁用**可适用的异常情况检测的单选按钮。可能的反常现象检测值如下：

•HTTP — HTTP定义了消息如何被格式化并且被传送，并且什么动作Web服务器和浏览器应该采取以回应多种命令。 使用此选项， Web攻击签名被匹配， UTF-8 (1， 2和3字节)代码由HTTP请求译码器解码，并且URI在模式匹配前是正常化的。

•FTP —文件传输协议(FTP)是用于的标准网络协议调用文件从一台主机或到另一台主机过渡基于TCP的网络，例如互联网。 FTP发现并且插入telnet opcodes到ftp命令流检测。

•TELNET — Telnet是使用访问远程计算机的一个user命令和TCP/IP协议。要执行此，它创建查找的本地设备的一个虚拟端口，好象直接地被连接到远端设备，允许两个设备之间的通信。

•RPC — Remote Procedure Call (RPC)是进程间通信(通常在另一个地址空间允许计算机程序造成子例行程序或程序执行的共享网络的另一台计算机)和不要求程序员对此远程交互作用明确地编码详细资料。 RPC记录fragges检测。




## 签名更新

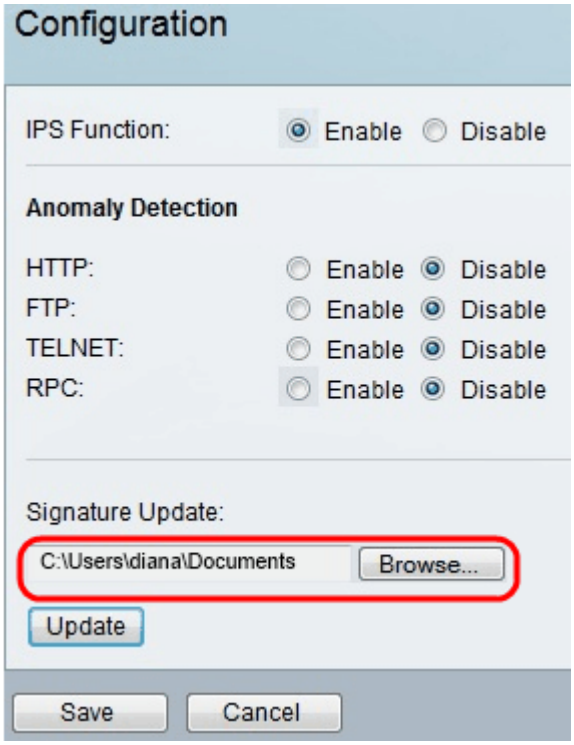
一基于签名的入侵防御系统监控匹配的网络流量对这些签名。一旦找到匹配入侵防御系统采取适当行为。

**Note:**在您升级签名文件前，从Cisco网站请获得路由器入侵防御系统(IPS)文件。要查找文件，请去www.cisco.com/go/software (需要的注册/登录)，并且搜索RVS4000。然后请抽出文件。

步骤1.登陆在Web配置工具并且选择**IPS > Configuration>签名更新**。

步骤2.登陆在Web配置工具并且选择IPS > Configuration>签名更新

步骤3.输入IPS签名文件名在签名更新字段或者点击访问查找文件。

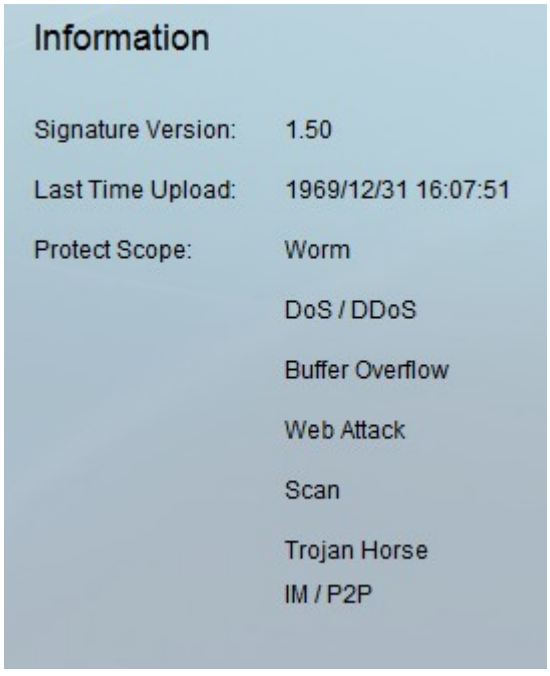



步骤4.点击**更新。**

步骤5.点击**"Save"**保存所有配置设置。

## IPS信息

步骤1.登陆在Web配置工具并且选择**IPS >信息**。信息页打开。




以下信息在IPS信息域显示。

- •签名版本—显示签名模式的版本在防止受到有恶意的威胁的路由器的。
- •上次加载—，当在路由器的签名模式是最近更新，这显示。
- •保护范围—列出路由器的IPS功能保护agains攻击的种类。

–病毒蠕虫—计算机蠕虫是在网络有能力复制自己的一个病毒代码。这感染每台计算机并且使用网络作为机制传播。

– DoS/DDoS —拒绝服务预防强化网络安全。DoS和DDoS攻击充斥网络与限制网络资源的可用性的另外的请求

–缓冲区溢出—缓冲区溢出攻击采取宫殿，当某一数据数量从程序或进程的在临时内存时存储，攻击网络和计算机的此数据包含病毒代码。

– Web攻击—是，当网站有攻击网络或设备的一个有恶意的文件。

–扫描—，当一个病毒代码被发送到在设备的端口测试其状态时，端口扫瞄攻击发生。攻击者用于此信息了解设备的缺点。

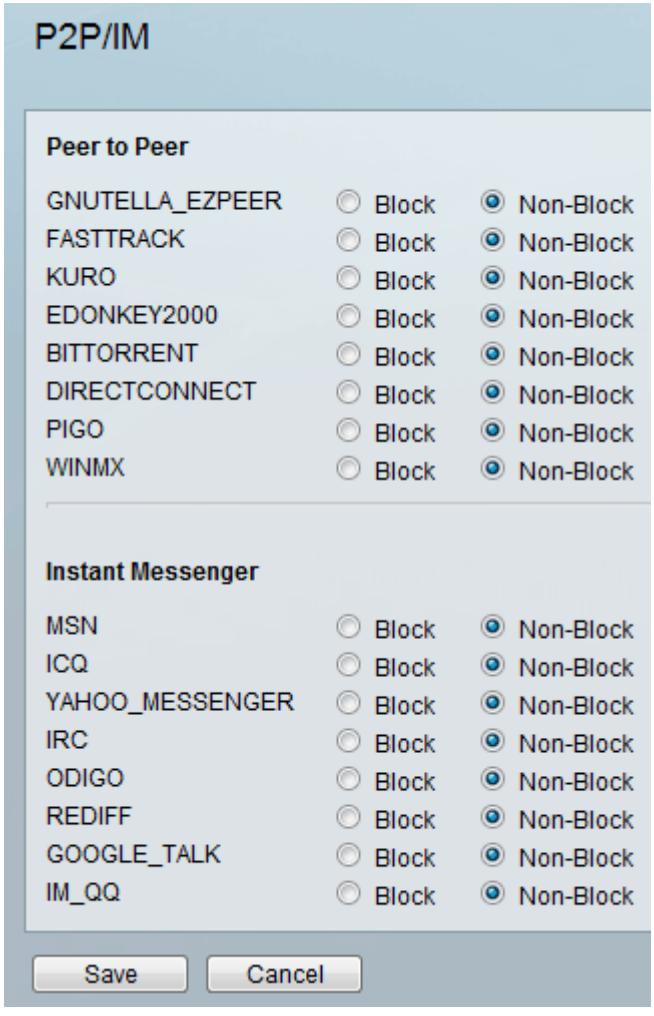
–病毒木马—电脑程式内的病毒或者特洛伊人，是在一个合法程序或文件隐藏的is is的一个病毒代码。当此文件或计划由用户时赞同，病毒代码攻击设备或网络。

– P2P —对等(P2P)网络类似于每台计算机作为服务器和客户端的客户端服务器网络。P2P攻击防止计算机之间的通信在网络导致信息丧失并且相冲突的网络。

– IM —即时消息攻击发生，当用户在聊天会话上立即收到一个病毒代码消息。此病毒代码攻击设备和网络。

## (IM)设置的对等(P2P)和即时消息

步骤1.登陆到Web配置工具并且选择**IPS > P2P/IM**。*P2P/IM*页打开：



Note:即时通讯用户将使用IM软件与其他人或调用的数据联络。

Step 2.要阻拦特定的P2P请服务或IM服务，点击**块**单选按钮。

第3.步。要允许特定P2P请服务或IM服务，点击非**块**单选按钮。

步骤4.点击“Save”应用更改。