查看关于WRVS4400N无线N千兆位安全路由器的入侵防御系统(IPS)报告

客观

入侵防御系统(IPS)保护您的网络服务，例如Web和即时消息，并且防止您可能的弱点，例如病毒、蠕虫和可能的背后检测安全漏洞代码。IPS监控有恶意或不需要的工作情况的网络流量，并且，如果发现攻击，丢弃那些恶意信息包保护网络，当数据流的其余穿过网络时。IPS允许您坚持当前在最新的威胁，以便有恶意或残损的数据流在实时被识别，准确地被分类，并且被终止。

此条款显示WRVS4400N为系统的当前弱点生成的报道，这产生您必要信息控制在网络的该问题。

可适用的设备

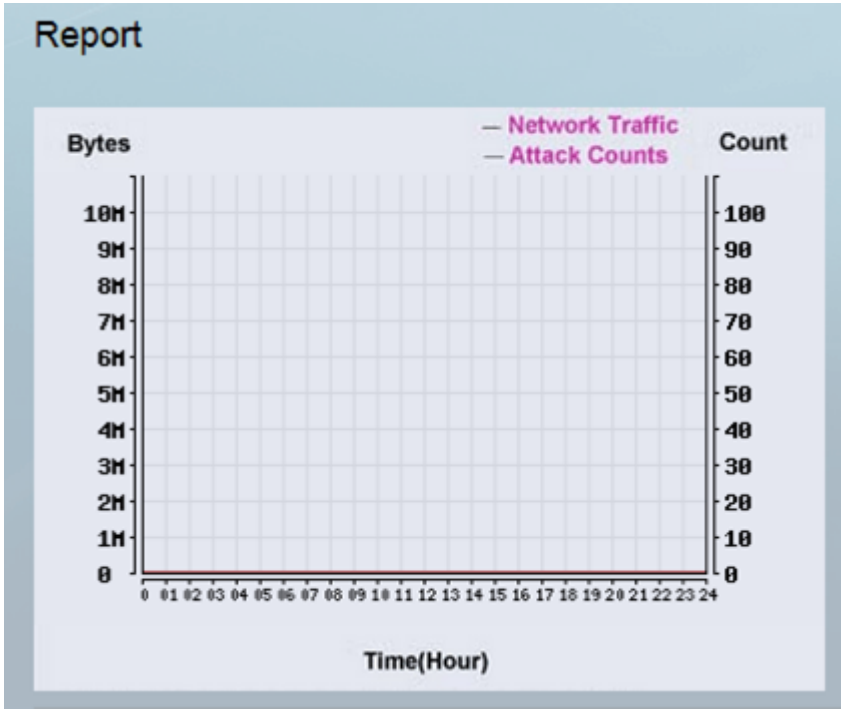
•WRVS4400N

软件版本

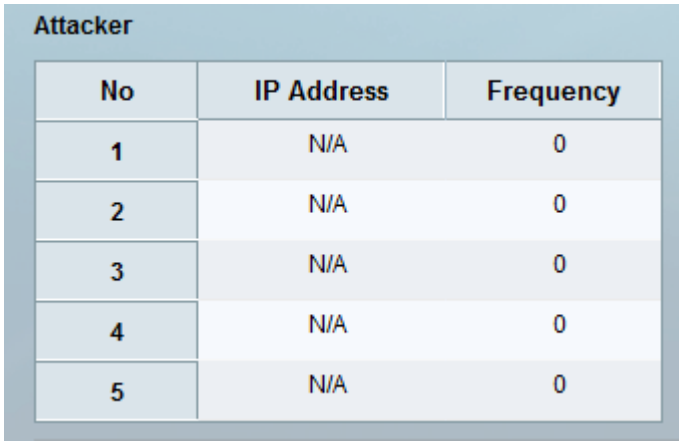
•v2.0.1.3

入侵防御系统报告

步骤1.登陆到Web配置工具并且选择**IPS >报告**。*报道*页打开。报告页显示三个部分报告，攻击者和被攻击的类别。



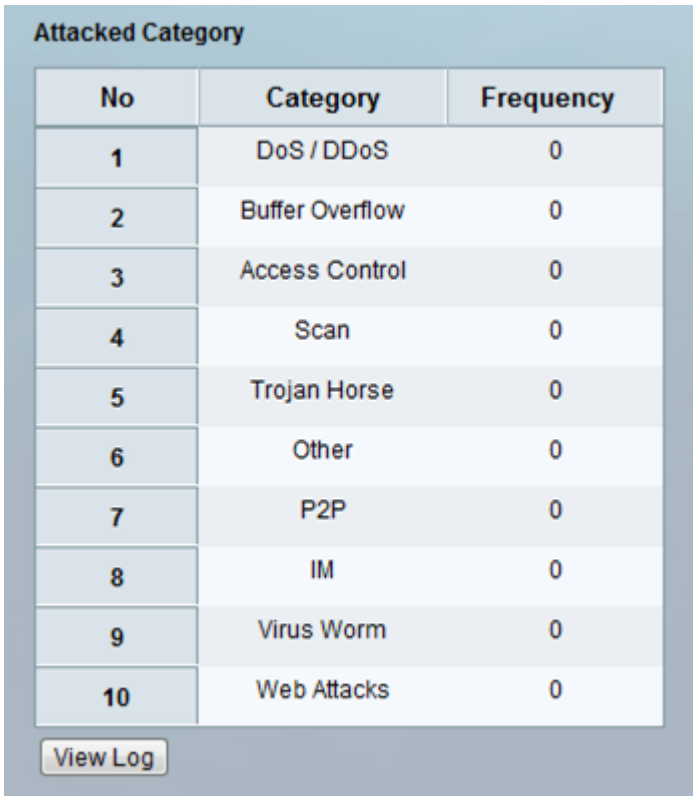
•报告图表—在前二十四小时内显示网络流量和攻击的数量的图形。



Attacker

No	IP Address	Frequency
1	N/A	0
2	N/A	0
3	N/A	0
4	N/A	0
5	N/A	0

•攻击者—显示攻击者的IP地址和他们在表里发生的次数。



Attacked Category

No	Category	Frequency
1	DoS / DDoS	0
2	Buffer Overflow	0
3	Access Control	0
4	Scan	0
5	Trojan Horse	0
6	Other	0
7	P2P	0
8	IM	0
9	Virus Worm	0
10	Web Attacks	0

View Log

•被攻击的类别—显示攻击的种类和在表里发生的次数。

– 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。

–访问控制—访问控制攻击发生，当访问控制的应用程序发生故障，并且可以中断访问数据进入到网络或设备。

–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。

–其他—网络或设备能遭受的其他攻击。

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

–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。

– Web攻击—是，当网站有攻击网络或设备的一个有恶意的文件。

步骤2.点击**View Log**按钮查看日志。这些是系统生成的消息，当网络受到攻击时。

- 编号NO-显示攻击在系统发生的次数。
- 当攻击发生了，定期显示时候
- 名字—显示攻击的名字
- 来源—显示攻击的来源

步骤3.点击**Clear按钮**收拾日志桌子。