

日志设置的配置在WRVS4400N千兆位安全路由器的

客观

日志是描述系统事件的一套消息。每个系统事件有不同的告警级别。日志在RAM、闪存和设备的一个远程日志服务器可以被保存本地。日志提供一个管理员戒备，当功能不正确地时运作，允许管理员采取行动更正他们。系统日志服务器能分离生成从系统的消息存储并且分析他们的软件。这节约生成日志设备的资源。

本文目标将显示您如何配置在WRVS4400N无线N千兆位安全路由器的日志设置。

可适用的设备

- WRVS4400N无线N千兆位安全路由器

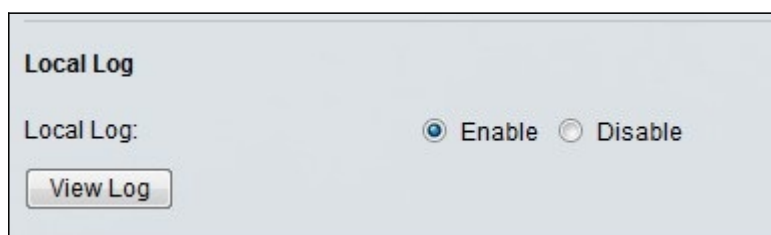
软件版本

- 2.0.1.3

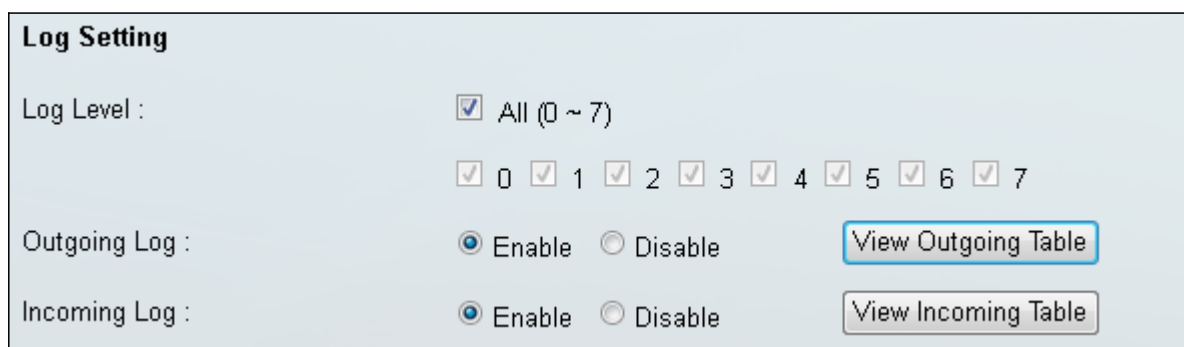
日志设置的配置

步骤1.登陆到Web配置工具并且选择Administration >日志。日志页打开：

Step 1.在本地日志地区中，请检查**Enable**单选按钮查看流出和流入日志。

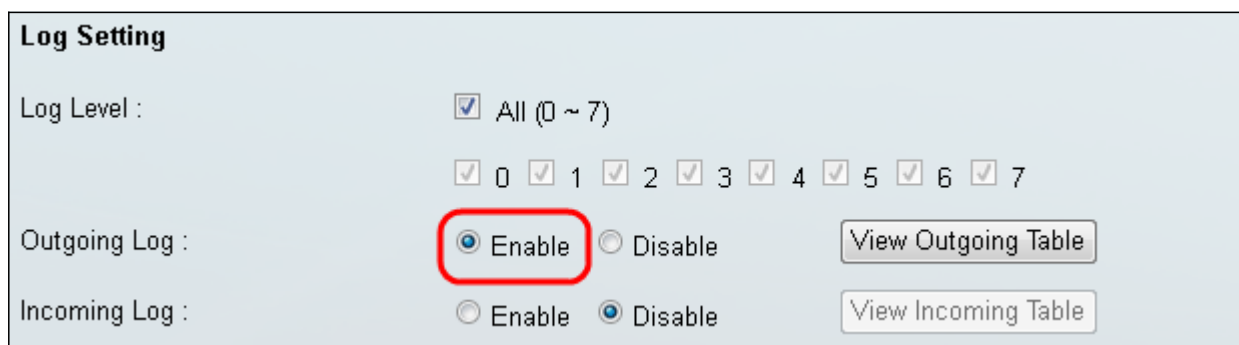


Step 2.检查**All**复选框或各自的(0,1,2,3,4,5,6,7个)级别复选框修改设备记录日志级别的设置。下列描述日志级别。



- 第7级—，当有不一致在网络时，传送调试信息。
- 第6级—发关于网络的当前状态的一个供参考消息。
- 第5级—传送信息，当网络正常时工作，但是有一个重要状况。
- 第4级—，当有问题情况在网络时，传送一个警告消息。
- 第3级—，当故障在网络时，发生了发一个错误信息。
- 第2级—，当一个严重情况是存在网络时，传送信息。
- 第1级—，当一个立即行动是需要的时，传送信息。
- 级别0 —，当系统是不可用的时，传送信息。

步骤3.点击在流出的日志字段的**Enable**单选按钮对enable (event)设备记录所有流出的信息包。



第4.步(可选)点击视图流出的表查看关于流出的信息包的信息包括来源IP、目的地IP和服务或端口号。

Log Setting

Log Level : All (0 ~ 7)

0 1 2 3 4 5 6 7

Outgoing Log : Enable Disable

Incoming Log : Enable Disable

流出的日志窗口打开

Outgoing Log

Total: 0 Current: 1 - 0

Dec 31 16:00:21 - br0: topology change detected, propagating
Dec 31 16:00:24 - download uses obsolete (PF_INET,SOCK_PACKET)

步骤5.点击在流入日志字段的**Enable**单选按钮对enable (event)设备记录所有流入信息包。

Log Setting

Log Level : All (0 ~ 7)

0 1 2 3 4 5 6 7

Outgoing Log : Enable Disable

Incoming Log : Enable Disable

第6步(可选)点击视图流入表查看关于流入信息包的信息包括来源IP、目的地IP和服务或端口号。

Log Setting

Log Level : All (0 ~ 7)

0 1 2 3 4 5 6 7

Outgoing Log : Enable Disable

Incoming Log : Enable Disable

流入日志窗口打开：

Incoming Log

Total: 0 Current: 1 - 0

Dec 31 16:00:26 - Trying to free free IRQ16
Dec 31 16:00:26 - Trying to free free IRQ17

步骤7.点击“Save”保存最后更改。

电子邮件告警

管理员用于电子邮件告警控制系统生成的日志。这些日志被发送到管理员能然后采取适当的行动的电子邮件。

步骤1.点击在电子邮件告警字段的**Enable**单选按钮。造成一个电子邮件立即发送这，如果发现DOS(拒绝服务)攻击。如果能够的话，请填写在剩余的字段的电子邮件地址信息在此部分。

Email Alerts

Email Alerts: Enable Disable

Denial of Service Thresholds: events (20 - 100)

Log Queue Length: entries (50 - 100)

Log Time Threshold: minutes (10 - 10,000)

SMTP Mail Server: Port:

Email Address for Alert Logs:

Return Email Address:

Enable SMTP Authentication

Username:

Password:

Step 2.在拒绝服务阈值字段，请输入的拒绝服务攻击的数量必须发现，在电子邮件被派出前。最小值是20。最大值是100。

第3步。在日志队列长度字段，在日志生成前，请输入条目的数量允许在队列。默认值是50个条目。

第4步。在日志时间阈值字段，请以分钟输入间隔，您希望电子邮件被发送。默认值是10分钟。

第5步。在SMTP邮件服务器领域，请输入您使用SMTP服务器的传出电子邮件的域名或IP地址。

第6步。在Port字段，请输入与此连接的SMTP服务器产生关联的端口。

第7步。在戒备日志字段，请输入日志被发送的电子邮件地址。

第8步。在回归电子邮件地址字段，请输入您希望出现作为发送方的地址的电子邮件地址。

第9步(可选)，如果您的SMTP服务器要求认证，检查Enable (event) SMTP认证复选框。

Email Alerts

Email Alerts: Enable Disable

Denial of Service Thresholds: 50 events (20 - 100)

Log Queue Length: 65 entries (50 - 100)

Log Time Threshold: 11 minutes (10 - 10,000)

SMTP Mail Server: 192.168.25.165 Port: 25

Email Address for Alert Logs: example.email@company.com

Return Email Address: example.email@company.com

Enable SMTP Authentication

Username: user.exp

Password: ●●●●

E-mail Log Now

节时：如果SMTP认证是失效的，请跳到第13步。

步骤10.输入用户名在用户名字段。这使用SMTP服务器的认证。

步骤11.输入密码在密码字段。这使用SMTP服务器的认证。

步骤12。(可选)测试电子邮件设置，**当前请点击电子邮件日志**。这造成日志立即被发电子邮件。

第13步。点击“**Save**”保存最后更改。

系统日志

步骤1.点击**Enable**单选按钮对enable (event) Syslog标准。

Syslog

Syslog: Enable Disable

Syslog Server: 192.168.45.89 (Name or IP Address)

步骤2.输入系统日志服务器的域名或IP地址在系统日志服务器领域。

步骤3.点击“**Save**”保存最后更改。

输出

输出信息组事件日志用于阻拦系统能生成的可能的消息，当固件不正常时运转。这为管理员是非常有用的，因为产生一次戒备，当设备不与早先固件一起使用时或，当固件出故障时。

步骤1.点击在**输出阻塞事件日志**字段的**Enable (event)**对enable (event)输出阻塞功能。

Output

Output Blocking Event Log: Enable Disable

步骤2. 点击“Save”保存最后更改。

本地日志

本地日志在网络用于管理员生成日志本地。

步骤1. 点击在本地日志字段的**Enable**单选按钮。这允许您查看所有流入和流出的日志日志。

Local Log

Local Log: Enable Disable

步骤2. 点击**View Log**按钮查看日志。

Local Log

Local Log: Enable Disable

所有日志窗口出现。这显示在路由器生成了的本地日志。

All Log

Type: ALL

```
Dec 31 16:00:07 - bind 0.0.0.0 - Address already in use
Dec 31 16:00:07 - started as root without requesting chroot(), warning only
Dec 31 16:00:07 - starting on , port 80
Dec 31 16:00:21 - br0: port 2(eth2) entering forwarding state
Dec 31 16:00:21 - br0: topology change detected, propagating
Dec 31 16:00:21 - br0: port 1(eth0) entering forwarding state
Dec 31 16:00:21 - br0: topology change detected, propagating
Dec 31 16:00:24 - download uses obsolete (PF_INET,SOCK_PACKET)
Dec 31 16:00:26 - Kris Linux Driver:Version=v2.00 for CISCO's RVSR000,WRVS4400N &
WRVS4400Nv2(Feb 18 2009:18:16:43)
Dec 31 16:00:26 - Enable Tcp Connection Tracking
Dec 31 16:00:26 - The Total Used Table Memory Size = 0xFB4878 = 16082K
Dec 31 16:00:26 - Trying to free free IRQ16
Dec 31 16:00:26 - Trying to free free IRQ17
Dec 31 16:00:27 - version 0.7.2 started
Dec 31 16:00:31 - Kris is unlocked
Dec 31 16:00:31 - Reset IDP Engine!!!
Dec 31 16:00:31 - The Total Used Table Memory Size = 0xFB4878 = 16082K
Dec 31 16:00:31 - Enable DDOS Detection!!
Dec 31 16:00:31 - Enable PortScan Detection!!
Dec 31 16:00:31 - Enable IP Sweep Detection!!
```


步骤3.点击“**Save**”保存日志设置。