

# 在RV220W和RV120W的远程记录配置

## 客观

远程和本地记录提供关于拒绝服务攻击、一般攻击、登录尝试、丢弃的数据包等等远程记录的信息是监控多台主机日志文件的其中一个方法。并且，用户也许在某些情况下要存储注册不是物理的可访问的分开的安全网络，这是，当远程记录进入使用时。

本文描述如何配置注册RV220W和RV120W的遥控。

## 可适用的设备

- RV220W
- RV120W

## 软件版本

- v1.0.4.17

## 配置远程记录

### 添加远程日志标识

添加一个远程日志标识与SMTP服务器一起使用并且用期望电子邮件配置日志设置。

步骤1. 登陆到Web配置工具并且选择**Administration > 记录 > 远程记录配置**。远程记录配置页打开：

## Remote Logging Configuration

### Log Options

Remote Log Identifier:

### E-Mail Logs Settings

E-Mail Logs:  Enable

E-Mail Server Address:

SMTP Port:  (Range: 1 - 65535, Default: 25)

Return E-Mail Address:

Send to E-Mail Address (1):

Send to E-Mail Address (2):  (Optional)

Send to E-Mail Address (3):  (Optional)

Authentication with SMTP Server:  ▾

Username:

Password:

Respond to Identd from SMTP Server:

步骤2.输入前缀添加到消息的来源的更加容易的证明的每日志消息在远程日志标识符字段的。日志标识将被添加到电子邮件和系统消息。

第3步：检查**电子邮件日志**复选框发送所有日志到下面被配置的电子邮件。

步骤4.输入简单邮件传输协议(SMTP)服务器的IP地址或互联网名称在电子邮件服务器地址地址字段。路由器将连接到此服务器发送电子邮件日志，当要求。

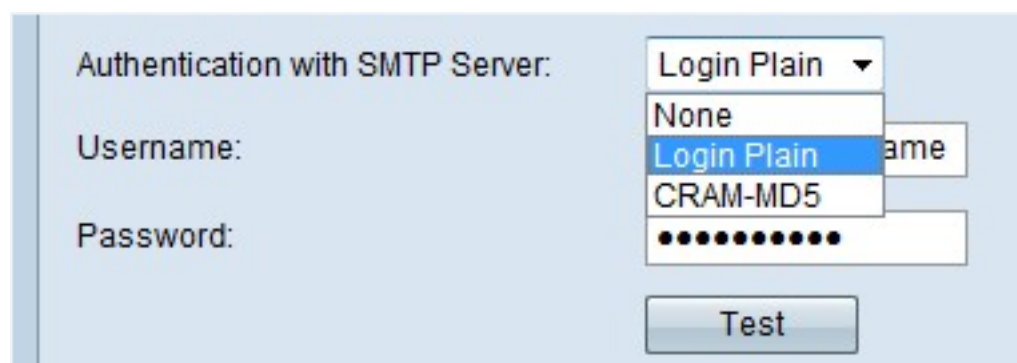
步骤5.输入用于的端口号连接到SMTP在Port字段的SMTP的服务器。

步骤6.输入SMTP服务器将使用发送在回归电子邮件地址字段的电子邮件的电子邮件地址。

步骤7.输入日志戒备将被发送在发送到电子邮件Address(1)字段的电子邮件地址。这是将发送日志戒备的电子邮件。

第8步(可选)输入日志戒备将被发送在发送到电子邮件Address(2)字段的电子邮件地址。这是将发送日志戒备的一个另外的电子邮件。

第9步(可选)输入日志戒备将被发送在发送到电子邮件Address(3)字段的电子邮件地址。这是将发送日志戒备的另一个另外的电子邮件。



The image shows a configuration window for SMTP authentication. On the left, there are labels for 'Authentication with SMTP Server:', 'Username:', and 'Password:'. To the right, a dropdown menu is open, showing options: 'Login Plain' (with a downward arrow), 'None', 'Login Plain' (highlighted in blue), 'CRAM-MD5', and a masked password field with ten dots. Below the dropdown is a 'Test' button.

步骤10.从与SMTP服务器下拉列表的认证选择所需的验证类型。

- 什么都—这禁用认证。
- 洛金无格式—，在接受连接前，这要求SMTP服务器验证。这是登陆的一个普通的方法对SMTP服务器。在用户名和密码从客户端被发送到服务器后，他们被结合对base64编码的字符串。用户名和密码没有被发送作为在互联网的纯文本，不同于MD5。
- CRAM-MD5 —，在接受连接前，这要求SMTP服务器验证。在CRAM-MD5认证，服务器首先发送一个挑战字符串到客户端，并且答复从客户端被收到作为字符串。此提供是安全的种类哈希不可以被复制没有其密码，其他不能重赛哈希，并且观察员没有了解一个的选项密码。

步骤11.输入将使用认证在用户名和密码字段的用户名和密码，如果洛金无格式或CRAM-MD5在第8.步被选择了。

步骤12. 点击**测试**验证正确地配置电子邮件日志功能。

第13步。检查**回应从SMTP服务器**复选框的**Identd**配置路由器回答自SMTP服务器的一个IDENTD请求。Ident协议是验证发送方(提供称为identd的ident服务的一个普通的守护程序程序电子邮件的方案)。

## 由日程表发送电子邮件日志

配置日程表这样日志被发电子邮件在日/星期的特定时间。可以如期望的一样配置记录的策略与日程表一起使用的时代。

步骤1.登陆到Web配置工具并且选择**Administration > 记录 > 远程记录配置**。远程记录配置页打开：

**Send E-Mail Logs by Schedule**

Unit:

Day:

Time:   
HH

Logging Policy:

**Syslog Server**

<input checked="" type="checkbox"/>	Syslog Server 1:	<input type="text" value="ExampleSyslog1"/>	Logging Policy:	<input type="text" value="default"/>
<input checked="" type="checkbox"/>	Syslog Server 2:	<input type="text" value="ExampleSyslog1"/>	Logging Policy:	<input type="text" value="default"/>
<input type="checkbox"/>	Syslog Server 3:	<input type="text"/>	Logging Policy:	<input type="text" value="default"/>
<input type="checkbox"/>	Syslog Server 4:	<input type="text"/>	Logging Policy:	<input type="text" value="default"/>
<input type="checkbox"/>	Syslog Server 5:	<input type="text"/>	Logging Policy:	<input type="text" value="default"/>
<input type="checkbox"/>	Syslog Server 6:	<input type="text"/>	Logging Policy:	<input type="text" value="default"/>
<input type="checkbox"/>	Syslog Server 7:	<input type="text"/>	Logging Policy:	<input type="text" value="default"/>
<input type="checkbox"/>	Syslog Server 8:	<input type="text"/>	Logging Policy:	<input type="text" value="default"/>

Unit:

Day:

Time:   
HH

步骤2.从频率的单元下拉列表选择期望单元电子邮件日志。

第3.步(可选), 如果每星期在第2步被选择了, 从频率的日下拉列表选择期望日电子邮件日志。

第4.步(可选), 如果每周或每日在第2步被选择了, 从时间下拉列表选择日的期望时期的特定时间(小时)电子邮件日志被发送。

步骤5.点击**配置记录策略**, 并且*Policies*页的记录打开:

## Logging Policies

Logging Policy Table	
<input type="checkbox"/>	Policy Name
<input type="checkbox"/>	default
<input type="button" value="Add"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

步骤6. 点击**添加**，并且添加/编辑记录策略配置页打开：

### Logging Policies

#### Add / Edit Logging Policy Configuration

Policy Name:

IPsec VPN Logs:  Enable

Severity	System	Kernel	Wireless
Emergency:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Alert:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Critical:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Error:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warning:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Information:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Debugging:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

步骤7. 送进首选策略名称在Policy Name字段。

第8.步。检查IPSec VPN日志复选框对enable (event)日志与IPsec协商有关。这些与用户空间日志有关。

第9.步。检查appropriate复选框在可变的严重性配置表里：

- 紧急状态—，当系统是不可用的以一个紧急情况状态时，这发送日志。类似影响多个apps/服务器/站点的“紧急”情况。当这发生，所有技术将被通知。

- 戒备**—，当立即行动是需要的时，这发送日志。需要立即更正因此这通知人员。此的示例是主要ISP连接的损失。
- 重要**—，当设备在严重情况，这发送日志。这些日志可以立即被修理，但是这些日志指示系统的主要的故障。此的示例是备份ISP连接的损失。这些日志处理在全局级别。
- 错误**—这发送适合于对误差条件的日志。这些日志指示一个严重问题，但是在不要求立即关注的类别。这些日志消息能被描述作为非紧急故障和需要被传递到开发人员或admins。每个错误日志需要是内给定时间间隔已处理。
- 警告**—这发送日志以警告情况。这是题头为一个潜在问题，但是对一个实际问题的不是一种回应。它是表明警告组件或应用程序不在一个理想的状态。这些消息是没有错误，然而征兆错误将出现，如果行动没有采取，例如，当文件系统是85%充分时。
- 通知**—这发送是正常的日志，但是有重要状况。这些日志不是类似误差条件。对这些日志消息的解决方案集是总结他们在电子邮件和给您的admins或开发人员发电子邮件察觉一个潜在问题，但是没有需要一个立即行动。
- 信息**—这发送有仅供参考消息的日志。这些日志消息包含admin不重要的信息，并且可以为文档问题进一步被收获。
- 调试**—这发送有仅调试消息的日志。这些日志是有用对开发人员调试应用程序，但是没有用在操作中。

步骤10.点击“Save”应用更改。

## 系统日志服务器

如果希望路由器发送日志到系统日志服务器，请配置以下。您能配置8个系统日志服务器。

步骤1.登陆到Web配置工具并且选择**Administration > 记录 > 远程记录配置**。远程记录配置页打开：

Checkbox	Server Name	Logging Policy
<input checked="" type="checkbox"/>	Syslog Server 1 ExamplePolicy 1	examplepolicy
<input type="checkbox"/>	Syslog Server 2 ExamplePolicy2	default
<input type="checkbox"/>	Syslog Server 3	default
<input type="checkbox"/>	Syslog Server 4	default
<input type="checkbox"/>	Syslog Server 5	default
<input type="checkbox"/>	Syslog Server 6	default
<input type="checkbox"/>	Syslog Server 7	default
<input type="checkbox"/>	Syslog Server 8	default

Buttons: Save, Cancel

**Step 2.**检查系统日志服务器复选框对enable (event) Syslog策略。

步骤3.输入服务器名在系统日志服务器1领域。

步骤4.从记录策略下拉列表选择策略。选项是从在记录添加的策略*Policies*页。

Steo 5.点击“**Save**”应用设置。