RV34x路由器上具有目标ACL限制的VLAN间路由

目标

本文介绍如何在RV34x系列路由器上使用目标访问控制列表(ACL)配置虚拟局域网间(VLAN)路由以限制某些流量。流量可以受IP地址、地址组或协议类型限制。

简介

VLAN非常出色，它们定义第2层网络中的广播域。广播域典型地以路由器分界，因为路由器不转发广播帧。2 层交换机基于它的配置来创建广播域。数据流不能在交换机内或两个交换机之间直接传递给另一个 VLAN（在两个广播域之间）。VLAN使您能够保持不同部门之间的独立。例如，您可能不希望销售部门与会计部门有任何关系。

独立性非常好，但是，如果您希望VLAN中的最终用户能够相互路由，情况会如何？销售部门可能需要向会计部门提交记录或时间表。会计部门可能希望向销售团队发送有关其工资或销售编号的通知。VLAN间路由就是这一天！

对于VLAN间通信，需要开放式系统互连(OSI)第3层设备（通常是路由器）。此第3层设备需要在每个VLAN接口中拥有一个Internet协议(IP)地址，并拥有到这些IP子网中每个子网的连接路由。然后，可以将每个IP子网中的主机配置为使用各自的VLAN接口IP地址作为其默认网关。配置后，最终用户可以向另一个VLAN中的最终用户发送消息。听起来很完美，对吧？

但是等等，那服务器在记帐中呢？该服务器上的敏感信息必须保持保护。别怕，这也有办法！RV34x系列路由器上的访问规则或策略允许配置规则以提高网络安全性。ACL是阻止或允许流量从特定用户发往或从特定用户发往的列表。访问规则可以配置为始终有效或基于已定义的计划。

本文将引导您完成配置第二个VLAN、VLAN间路由和ACL的步骤。

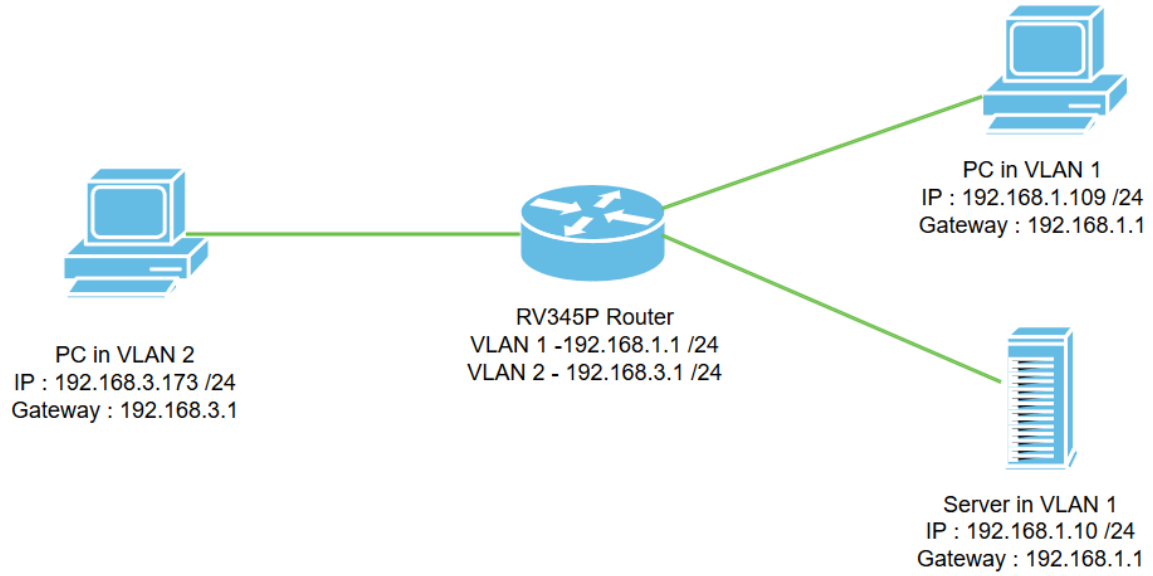
适用设备

- RV340
- RV340W
- RV345
- RV345P

软件版本

- 1.0.03.16

拓扑



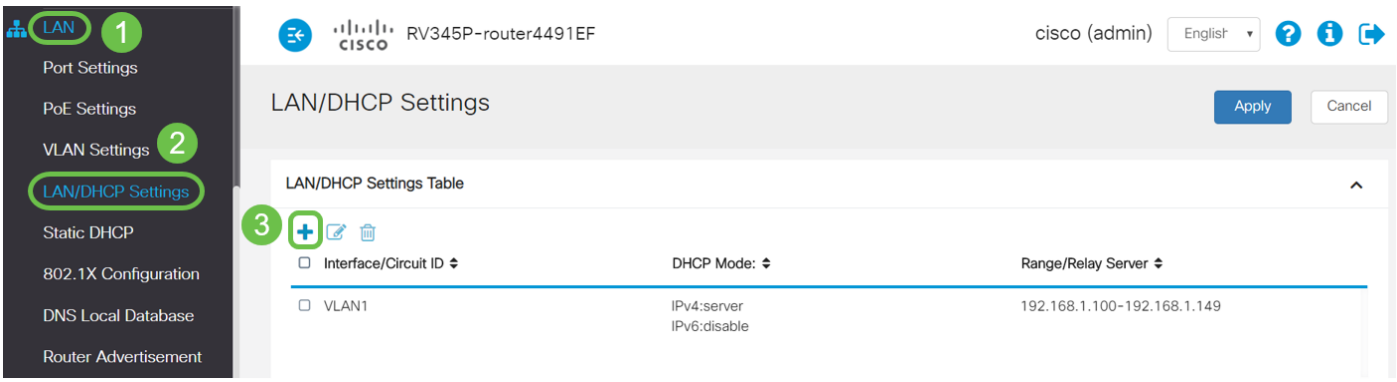
在此场景中，VLAN1和VLAN2都将启用VLAN间路由，以便这些VLAN中的用户能够相互通信。作为一项安全措施，我们将阻止VLAN2用户访问VLAN1服务器[Internet协议版本4(IPv4):192.168.1.10 /24]。

使用的路由器端口：

- VLAN1中的个人计算机(PC)连接在LAN1*端口*上。
- VLAN2中的个人计算机(PC)连接在LAN2*的端*口上。
- VLAN1中的服务器连接在LAN3*端口*上。

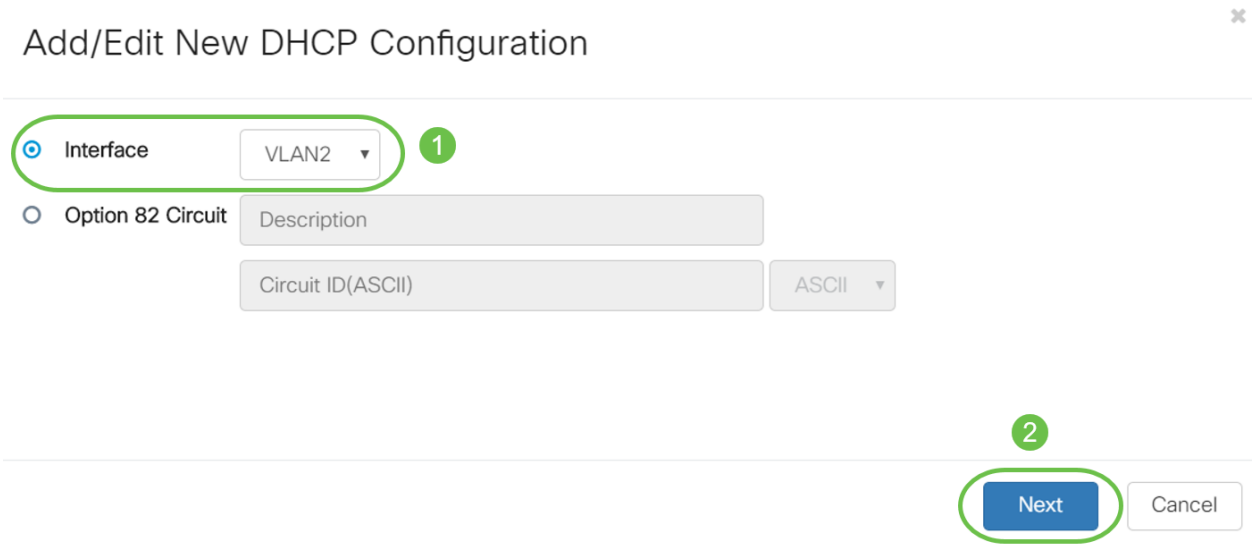
配置

步骤1.登录路由器的Web配置实用程序。要在路由器上添加新的VLAN接口，请导航至**LAN > LAN/DHCP Settings**，然后单击**LAN/DHCP Settings Table**下的加号图标。

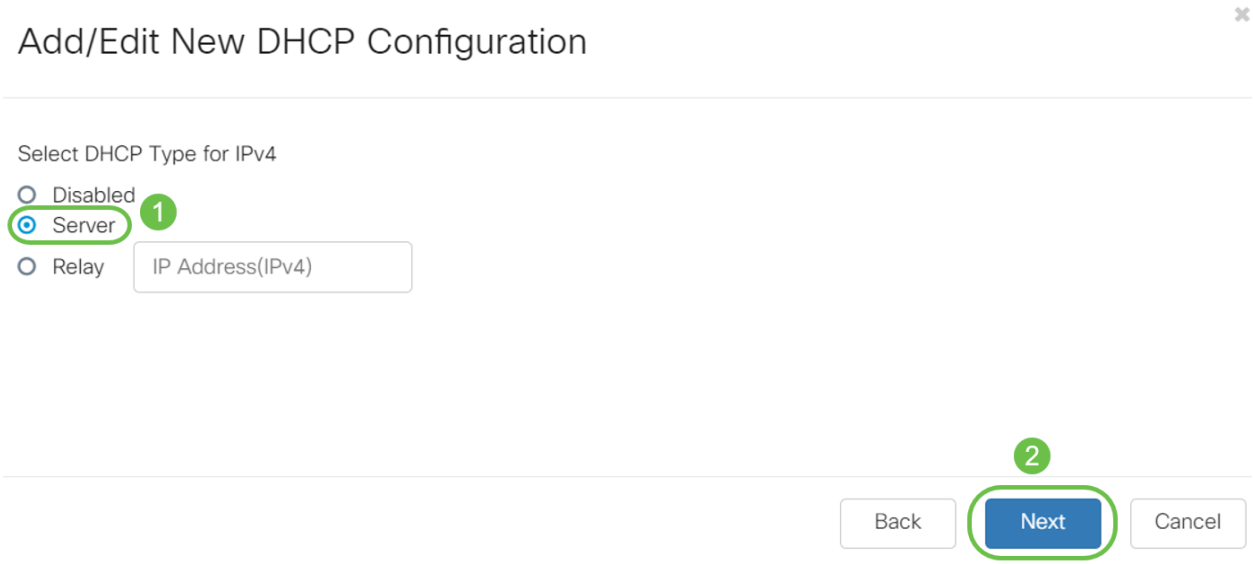


注意：默认情况下，VLAN1接口在RV34x路由器上创建，并且IPv4的动态主机配置协议(DHCP)服务器在该路由器上启用。

步骤2.将打开一个新的弹出窗口，其中已选*择VLAN2***接口**，单击**下一步**。



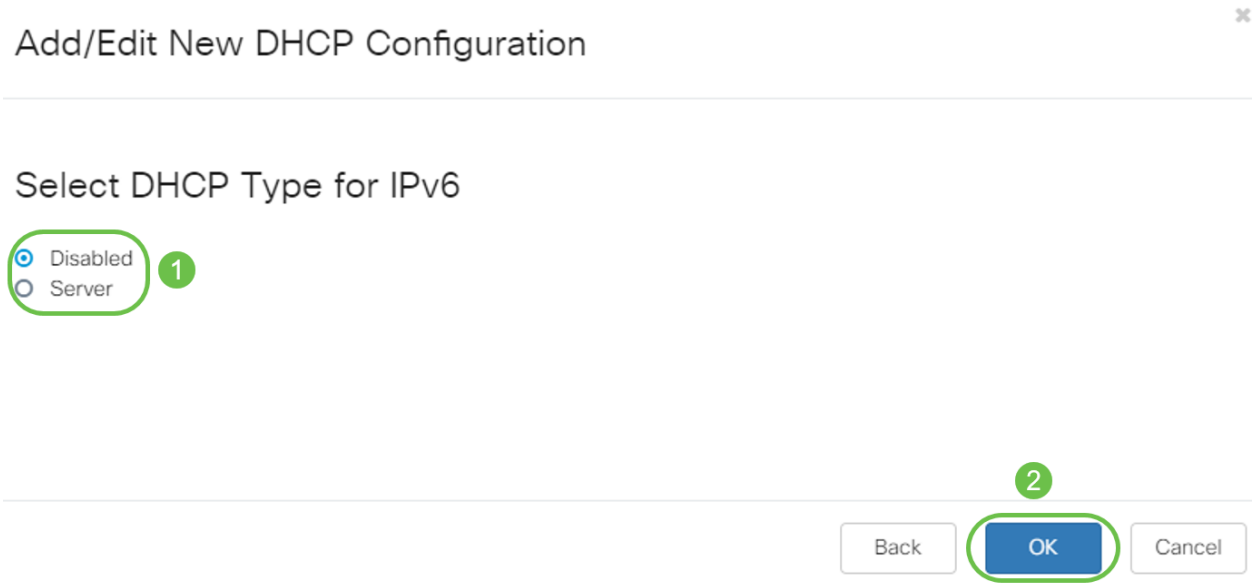
步骤3.要在VLAN2接口上启用DHCP服务器，请在“为IPv4选择*DHCP类型”下选择“服务器*”**下方**。单击 **Next**。



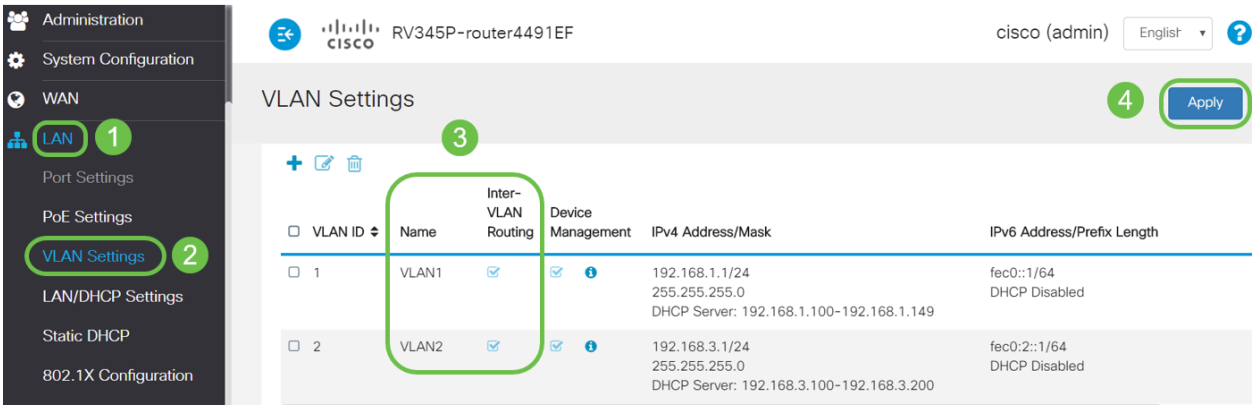
步骤4.输入DHCP服务器配置参数，包括*客户端租用时间*、*范围开始*、*范*围结束和*DNS服务器*。单击 **Next**。

步骤5.（可选）您可以通过选中**禁用**复选框来禁用*IPv6的DHCP类型，因为此示例基于IPv4。单击***确定**。DHCP服务器配置已完成。

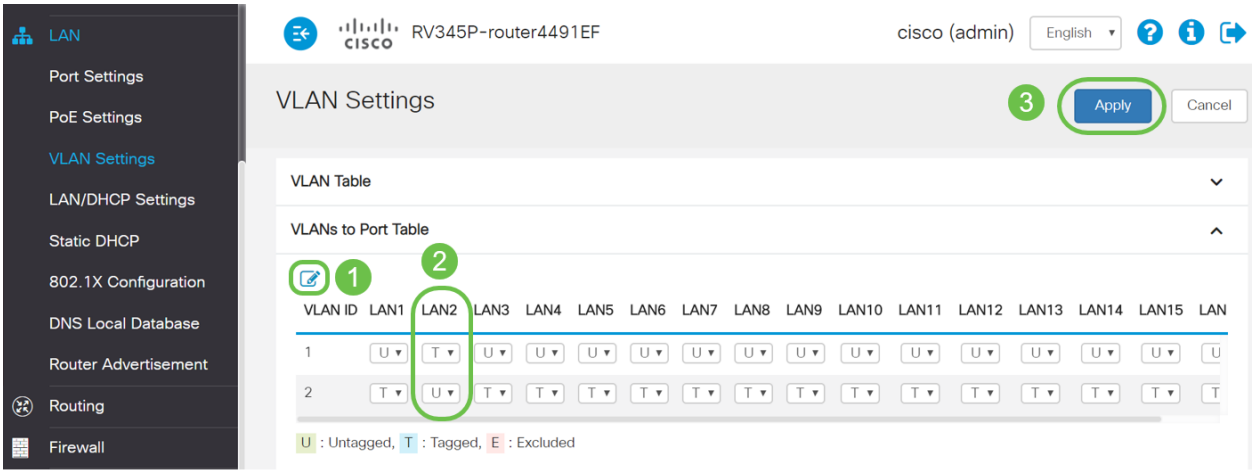
注意：您可以使用IPv6。



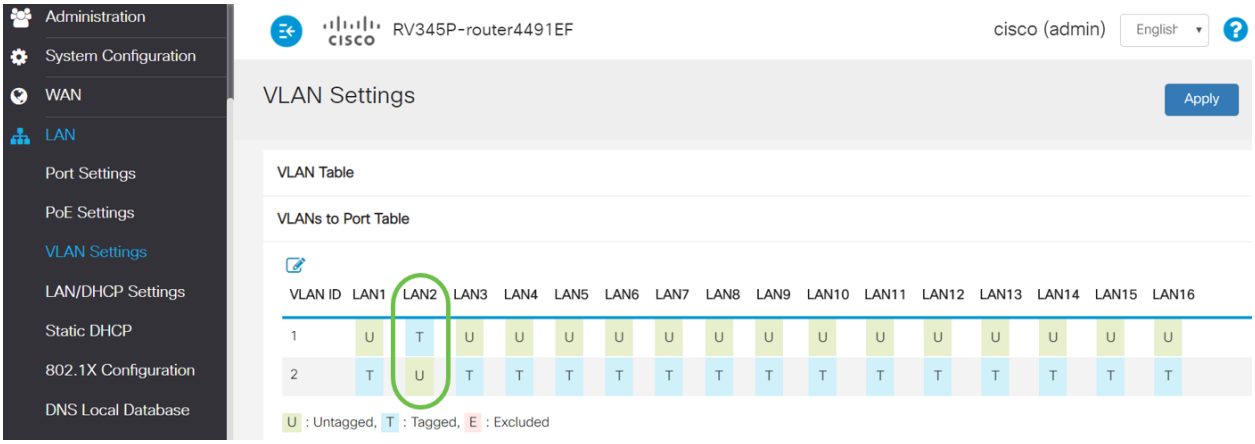
步骤6.导航到**LAN > VLAN Settings**，并验证*VLAN间路由*是否已为VLAN、VLAN1和VLAN2启用。此配置将启用两个VLAN之间的通信。单击 **Apply**。



步骤7.要在LAN2端口上为VLAN2分配无标*记的*流量，请单击“VLAN到端口表”选项*下的编辑*按钮。现在，在LAN2端口下，从下拉菜单中选择**VLAN1**的T（标记）选项和**VLAN2的U**（未标记）选项。单击**Apply**以保存配置。此配置将转发LAN2端口上VLAN2的无标记流量，以便PC网络接口卡(NIC)（通常不能进行VLAN标记）可以从VLAN2获取DHCP IP，并成为VLAN2的一部分。

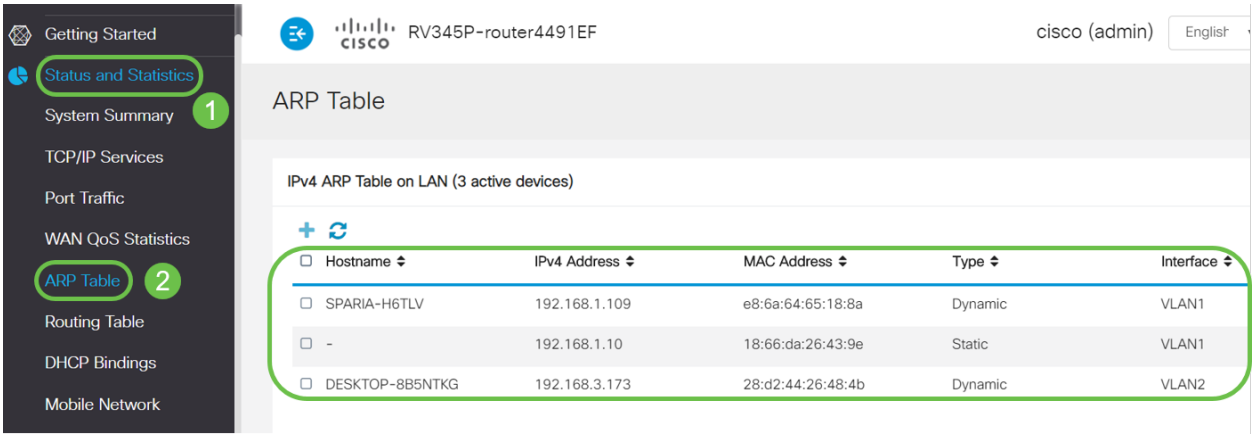


步骤8.检验LAN2端口的VLAN2设*置是*否显示为U（*无标记*）。 对于其余LAN端口，VLAN2设*置将为T*（已标记），VLAN1流量*将为U*（*未标记*）。

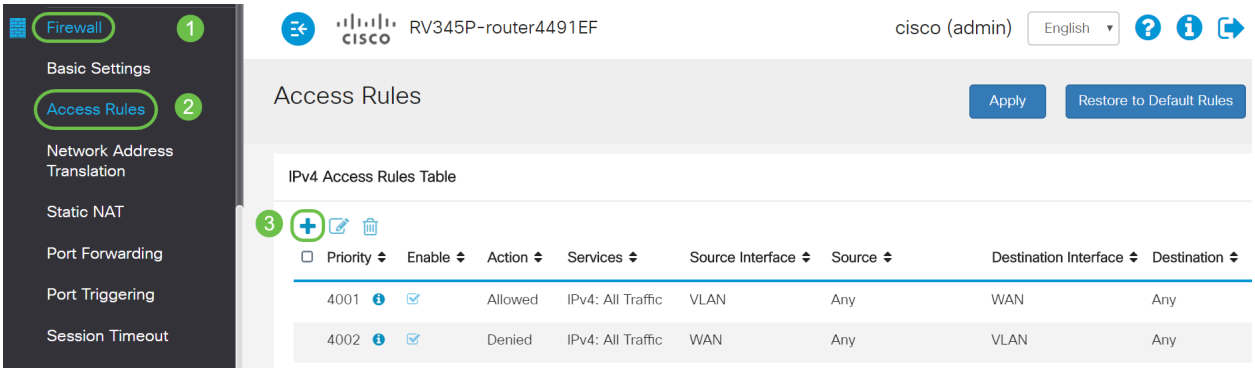


步骤9.导航至**Status and Statistics > ARP Table,**并验证PC的*动态IPv4*地址是否位于不同的VLAN中。

注意：VLAN1上的服务器IP已静态分配。



步骤10.应用ACL以限制服务器(IPv4:192.168.1.10/24)从VLAN2用户访问。要配置ACL，请导航至**Firewall > Access Rules**，然后单击加**号图**标以添加新规则。



步骤11.配置Access *Rules*参数。对于此方案，参数如下：

规则状态：enable

操作：拒绝

服务：所有通信

日志：真

来源接口:VLAN2

源地址：any

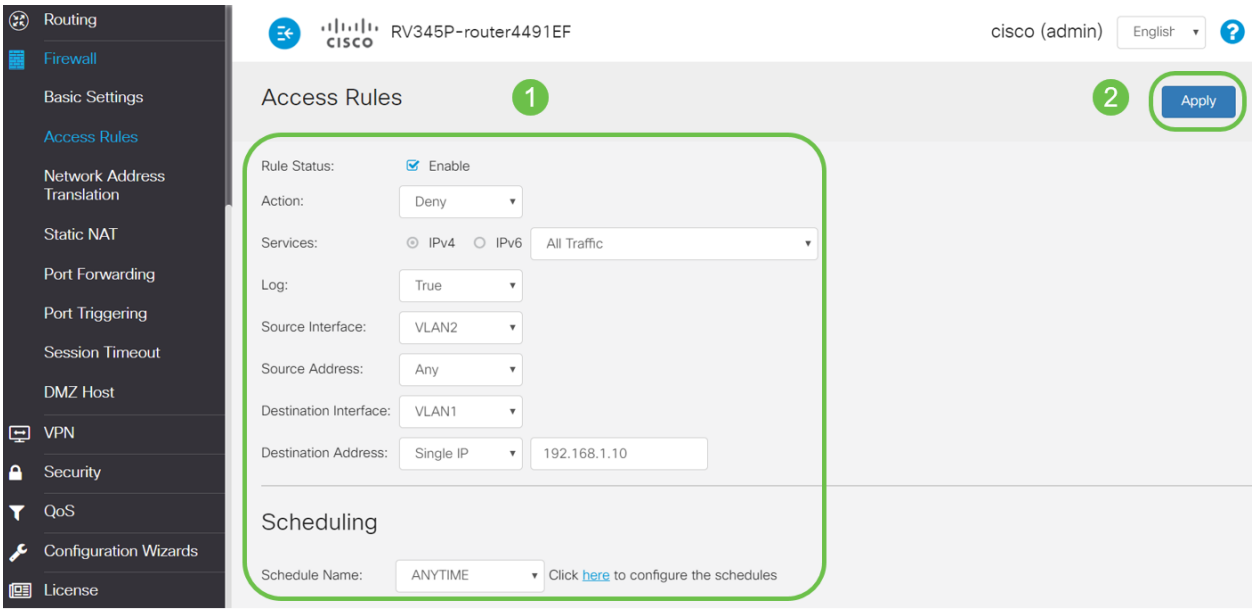
目标接口：VLAN1

目的地址：单IP 192.168.1.10

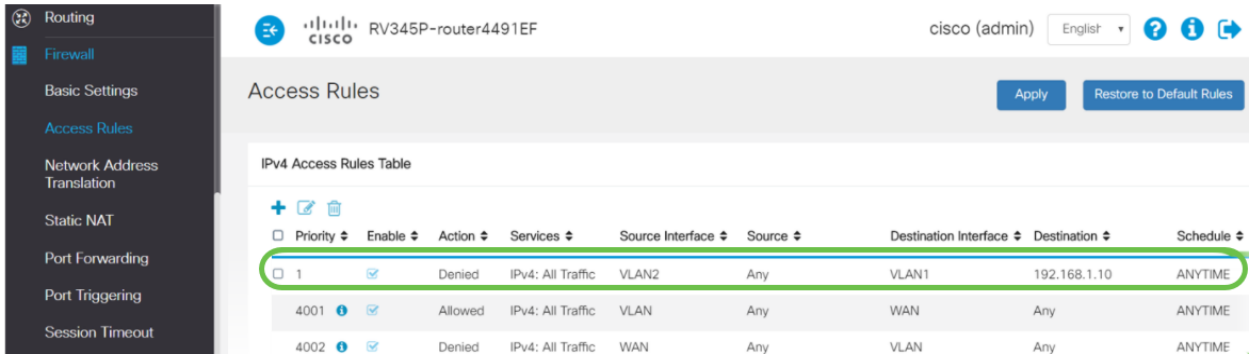
计划名称：随时

单击 **Apply**。

注意：在本例中，我们拒绝从VLAN2访问任何设备到服务器，然后允许访问VLAN1中的其他设备。您的需求可能有所不同。



步骤12. Access Rules*列表*将显示如下：



访问规则被明确定义，以限制服务器192.168.1.10从VLAN2用户访问。

确认

要检验服务，请打开命令提示符。在Windows平台上，单击Windows按钮，然后在计算机左下角的搜索框中键入**cmd**，然后从菜单中选择**Command Prompt**，即可实现**此目**标。

输入以下命令：

- 在VLAN2中的PC(192.168.3.173)上，对服务器(IP:192.168.1.10)。 您将收到“请*求超时*”通知，这意味着不允许通信。
- 在VLAN2中的PC(192.168.3.173)上，对VLAN1中的另一台PC(192.168.1.109)执行ping操作。您将获得成功的应答。

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

结论

您已经看到在RV34x系列路由器上配置VLAN间路由的必要步骤，以及如何执行目标ACL限制。现在，您可以利用所有这些知识，在您的网络中创建符合您需求的VLAN!