RV34x系列路由器上的ACL最佳实践

目标

本文的目的是介绍使用RV34x系列路由器创建访问控制列表(ACL)的最佳实践。

适用设备 |固件版本

- RV340 | 1.0.03.20 **（下载最新）**
- RV340W | 1.0.03.20 **（下载最新）**
- RV345 | 1.0.03.20 **（下载最新）**
- RV345P | 1.0.03.20 **（下载最新）**

简介

是否希望对网络进行更多控制？是否要采取额外步骤来确保网络安全？如果是，则访问控制列表(ACL)可能正是您需要的。

ACL由一个或多个集中定义网络流量配置文件的访问控制条目(ACE)组成。然后，思科软件功能（如流量过滤、优先级或自定义队列）可以引用此配置文件。每个ACL都包括一个操作元素（允许或拒绝）和一个基于源地址、目的地址、协议和协议特定参数等标准的过滤元素。

根据您输入的条件，您可以控制某些流量进入和/或离开网络。当路由器收到数据包时，它会检查数据包，以根据您的访问列表确定是转发还是丢弃数据包。

实施此安全级别时，会根据考虑特定网络场景和安全需求的不同使用案例。

请注意，路由器可以根据路由器上的配置自动创建访问列表。在这种情况下，您可能会看到访问列表，除非更改路由器配置，否则您无法清除这些列表。

为什么使用访问列表

- 在大多数情况下，我们使用ACL来提供基本的网络安全级别。例如，如果不配置ACL，默认情况下允许通过路由器的所有数据包发往网络的所有部分。
- ACL可允许一台主机、IP地址范围或网络，并防止另一台主机、IP地址范围或网络访问同一区域（主机或网络）。
- 通过使用ACL，您可以决定在路由器接口转发或阻止的流量类型。例如，您可以允许安全外壳(SSH)文件传输协议(SFTP)流量，同时阻止所有会话初始协议(SIP)流量。

何时使用访问列表

- 您应该在位于内部网络和外部网络（如Internet）之间的路由器中配置ACL。
- 您可以使用ACL控制进出内部网络特定部分的流量。
- 当您需要过滤入站流量或出站流量或同时过滤接口上的出站流量时。

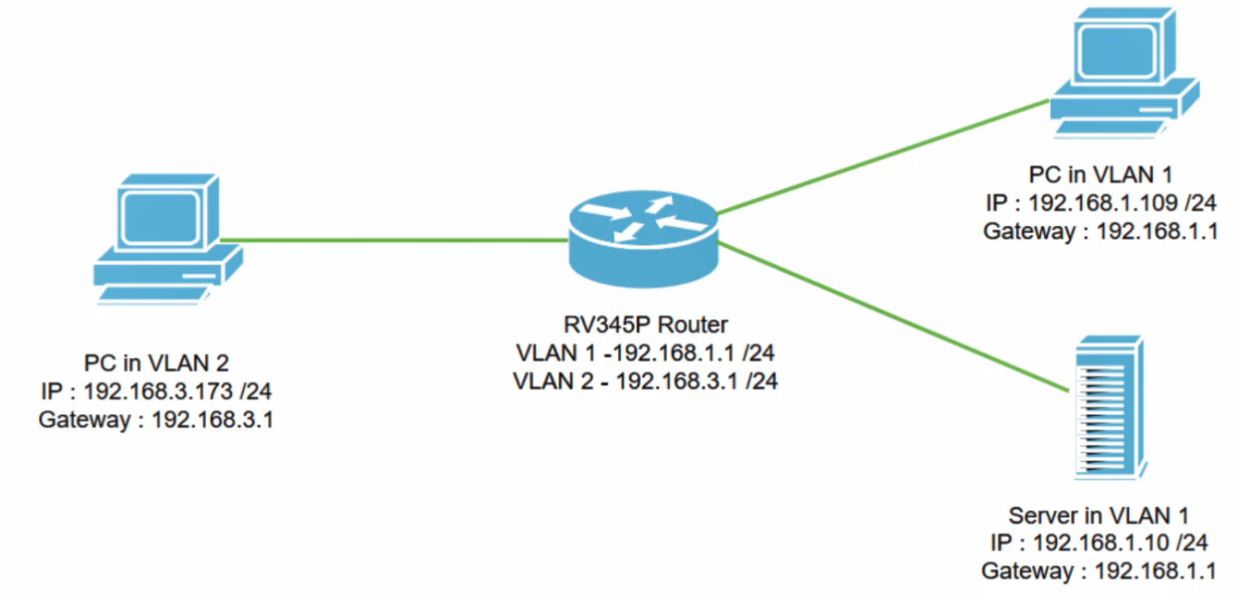
- 您应按协议定义ACL以控制流量。

使用访问列表配置基本安全的最佳实践

- 实施ACL，仅允许拒绝其他所有协议、端口和IP地址。
- 阻止声称具有相同目的地址和源地址的传入数据包（路由器自身受到陆地攻击）。
- 对内部（受信任）系统日志主机启用ACL的日志记录功能。
- 如果在路由器上使用简单网络管理协议(SNMP)，则必须配置SNMP ACL和复杂SNMP社区字符串。
- 仅允许内部地址从内部接口进入路由器，并仅允许发往内部地址的流量从外部（外部接口）进入路由器。
- 阻止组播（如果未使用）。
- 阻止某些互联网控制消息协议(ICMP)消息类型（重定向、回应）。
- 请始终考虑输入ACL的顺序。例如，当路由器决定是转发还是阻止数据包时，它会按照ACL的创建顺序根据每条ACL语句测试数据包。

在Cisco RV34x系列路由器中实施访问列表

网络拓扑示例



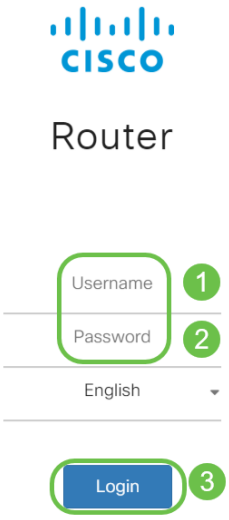
示例 情景

在此场景中，我们将复制此网络图，其中我们有一台RV345P路由器和两个不同的VLAN接口。VLAN 1和VLAN2中有一台PC，VLAN 1中也有一台服务器。VLAN间路由已启用，因此VLAN 1和VLAN 2用户能够相互通信。现在，我们将应用访问规则，以限制VLAN 2用户与VLAN 1中此服务器之间的通信。

配置示例

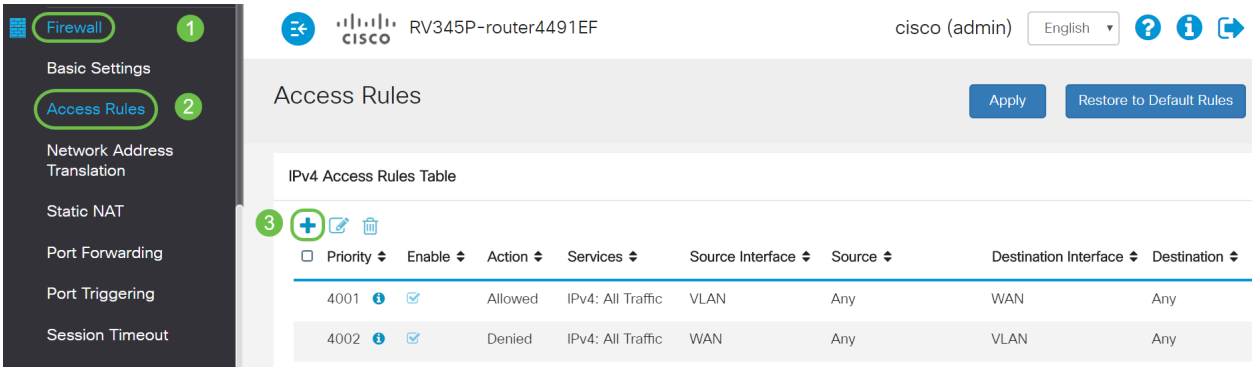
第 1 步

使用您配置的凭证登录路由器的Web用户界面(UI)。



步骤 2

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。



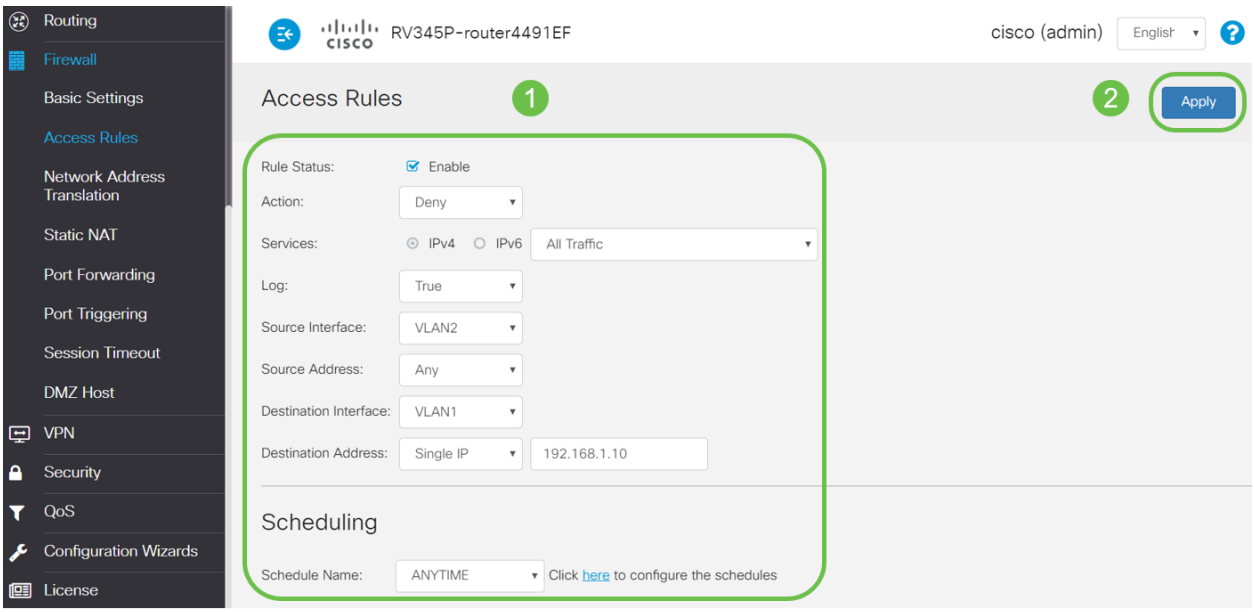
步骤 3

配置访*问规则*参数。应用ACL以限制服务器(IPv4:192.168.1.10/24)从VLAN2用户访问。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*

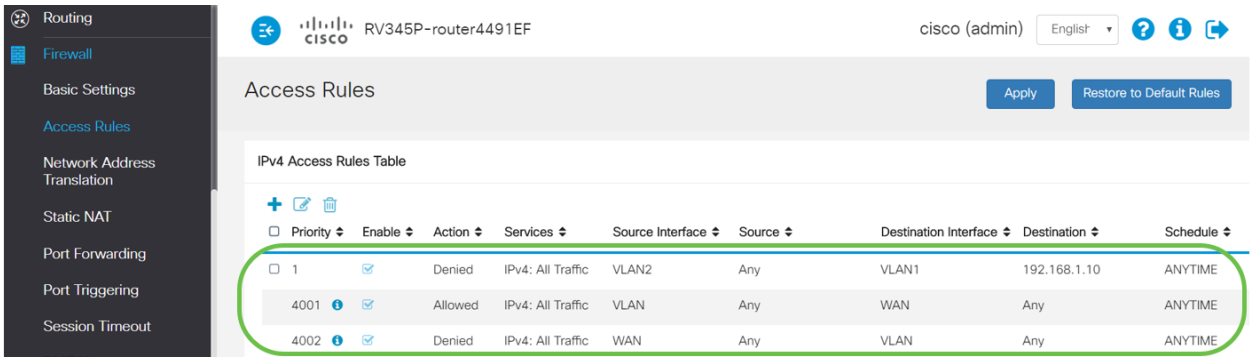
单击 **Apply**。

在本例中，我们拒绝从任何设备从VLAN2访问服务器，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 4

"访*问规则*"列表将显示如下：



确认

要检验服务，请打开命令提示符。在Windows平台上，可通过单击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**来实现此**操作**。

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
```

结论

您已看到在Cisco RV34x系列路由器上配置访问规则的必要步骤。现在，您可以应用该规则在您的网络中创建符合您需求的访问规则！