帶有目標ACL限制的RV34x路由器上的VLAN間路由

目標

本文介紹如何在具有目標訪問控制清單(ACL)的RV34x系列路由器上配置虛擬區域網(VLAN)間路由以限制某些流量。流量可以按IP地址、一組地址或協定型別進行限制。

簡介

VLAN非常棒，它們在第2層網路中定義廣播域。由於路由器不轉發廣播幀，因此廣播域通常由路由器限定。第2層交換機根據交換機的配置建立廣播域。流量無法直接傳遞到交換機內或兩台交換機之間的另一個VLAN（在廣播域之間）。VLAN使您能夠讓不同的部門彼此獨立。例如，您可能不希望銷售部門參與會計部門。

獨立性非常棒，但是如果您希望VLAN中的終端使用者能夠在彼此之間路由，該怎麼辦？銷售部門可能需要向會計部門提交記錄或時間表。會計部門可能需要向銷售團隊傳送有關其工資單或銷售編號的通知。這就是VLAN間路由節省時間的時候！

對於VLAN間通訊，需要開放系統互連(OSI)第3層裝置，通常是路由器。此第3層裝置需要在每個VLAN介面中具有一個Internet協定(IP)地址，並且擁有到這些IP子網的已連線路由。然後，可以將每個IP子網中的主機配置為使用各自的VLAN介面IP地址作為其預設網關。設定完成後，終端使用者可以向另一個VLAN中的終端使用者傳送訊息。聽起來很完美，對吧？

但是等等，伺服器在會計方面呢？該伺服器上有必須保持受保護的敏感資訊。不要害怕，這也有解決辦法！RV34x系列路由器上的訪問規則或策略允許配置規則以提高網路安全性。ACL是阻止或允許將流量傳送到特定使用者或從特定使用者處傳送的清單。可以將Access Rules配置為始終生效或基於定義的計畫。

本文將引導您完成配置第二個VLAN、VLAN間路由和ACL的步驟。

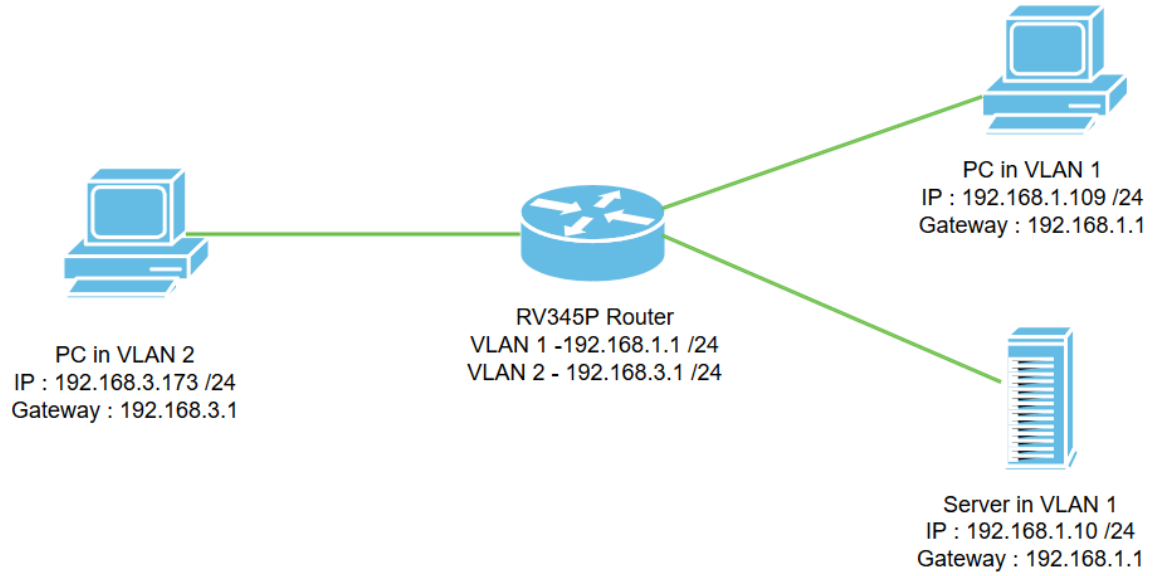
適用裝置

- RV340
- RV340W
- RV345
- RV345P

軟體版本

- 1.0.03.16

拓撲



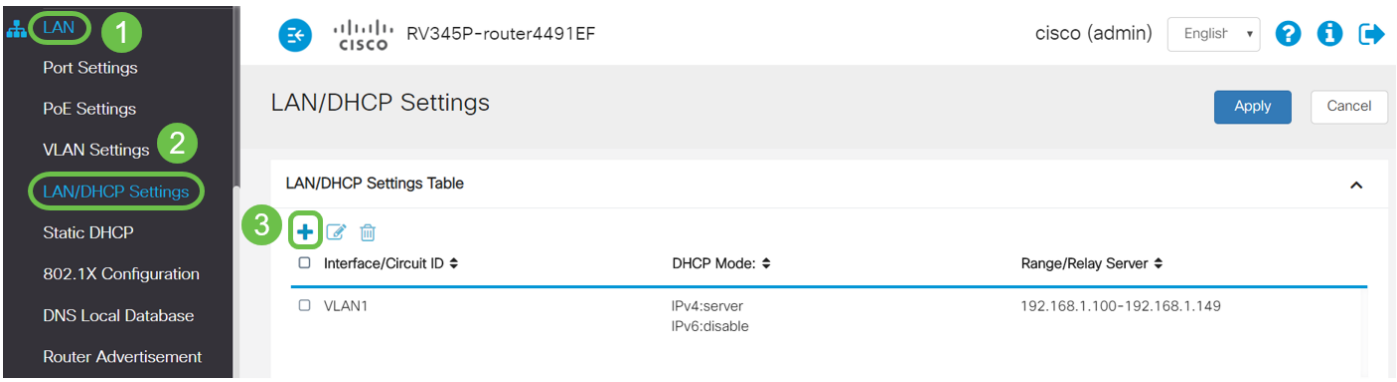
在此案例中，將同時為VLAN1和VLAN2啟用VLAN間路由，以便這些VLAN中的使用者可以彼此通訊。作為一項安全措施，我們將阻止VLAN2使用者訪問VLAN1伺服器[網際網路協定第4版(IPv4):192.168.1.10 /24]。

使用的路由器埠：

- VLAN1中的個人電腦(PC)連線到*LAN1端*口。
- VLAN2中的個人電腦(PC)連線到*LAN2端*口。
- VLAN1中的伺服器連線到*LAN3端*口。

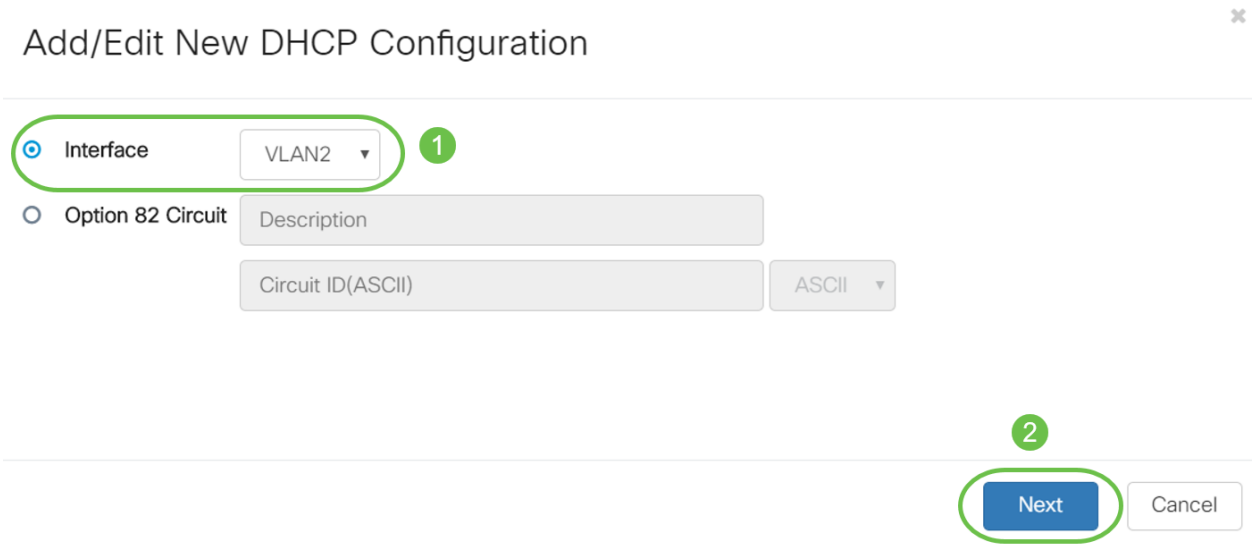
組態

步驟1.登入到路由器的Web配置實用程式。要在路由器上新增新的VLAN介面，請導航到**LAN > LAN/DHCP Settings**，然後按一下**LAN/DHCP Settings Table**下的**plus圖示**。

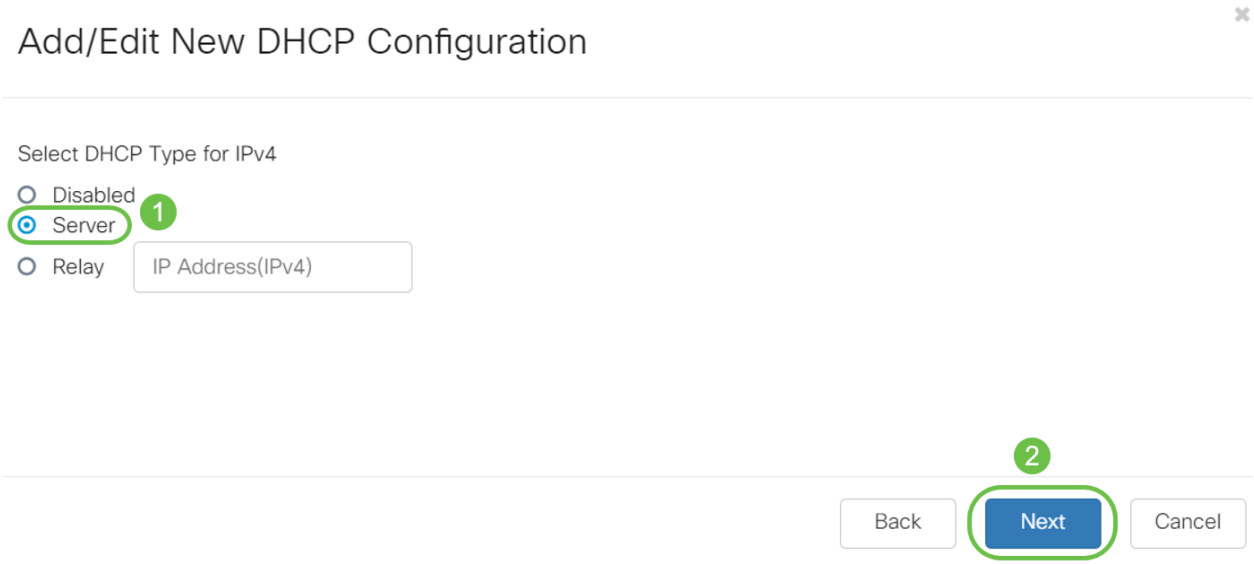


附註：VLAN1介面預設在RV34x路由器上建立，並且在該路由器上啟用了IPv4的動態主機配置協定(DHCP)伺服器。

步驟2.將開啟一個新的彈出視窗，選中*VLAN2接*口，按一下下**一步**。



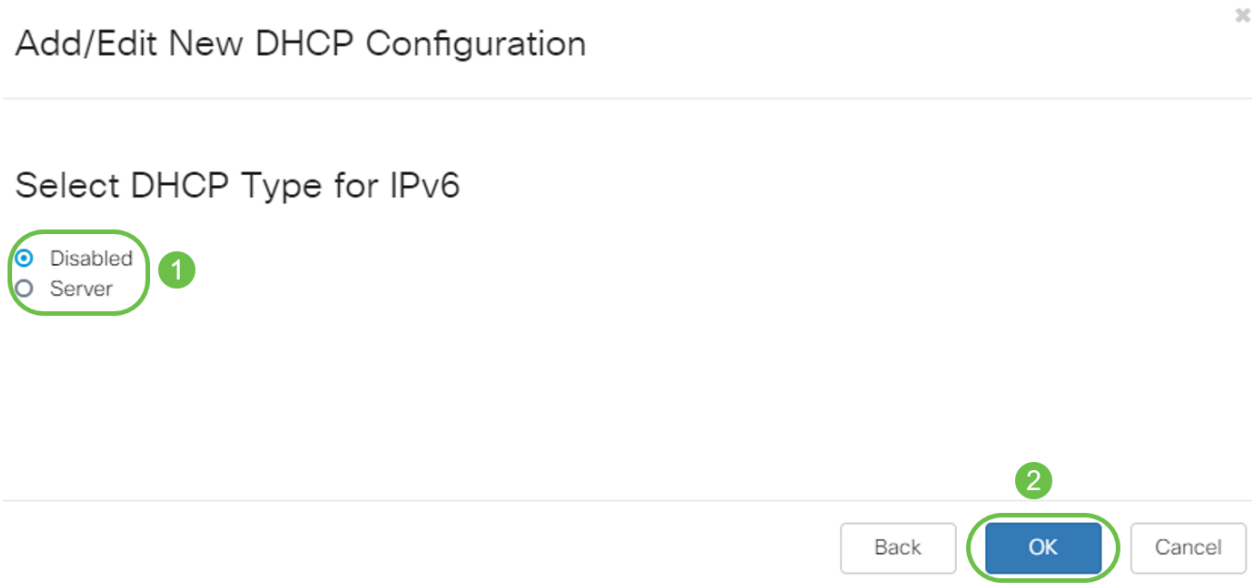
步驟3.要在VLAN2介面上啟用DHCP伺服器，請在*Select DHCP Type for IPv4*下，選擇**Server**。按「**Next**」（下一步）。



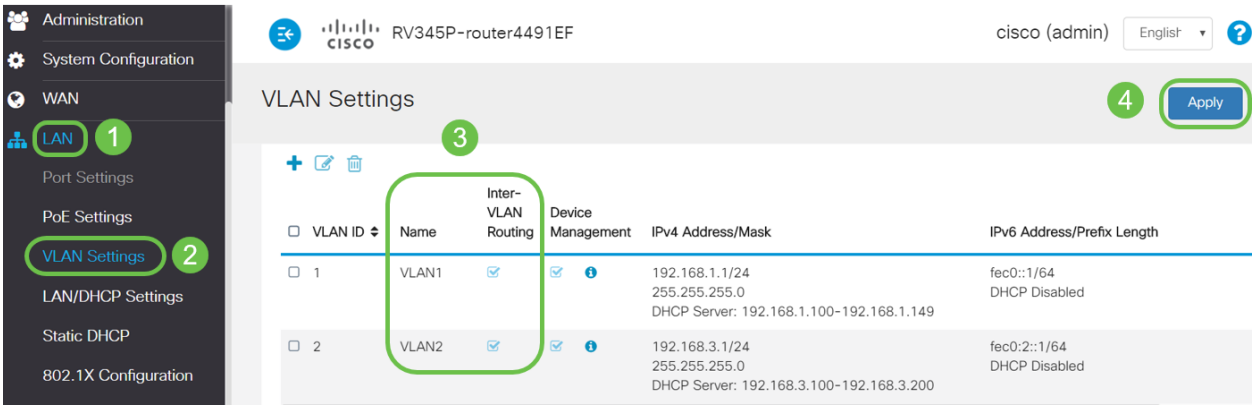
步驟4.輸入DHCP伺服器配置引數，包括*客戶端租用時間*、*範圍開始*、*範圍結束*和*DNS伺服器*。按「**Next**」（下一步）。

步驟5.（可選）您可以通過選中**Disabled**覈取方塊禁用IPv6的*DHCP型別，因為此示例基於IPv4。按一下***OK**。DHCP伺服器配置已完成。

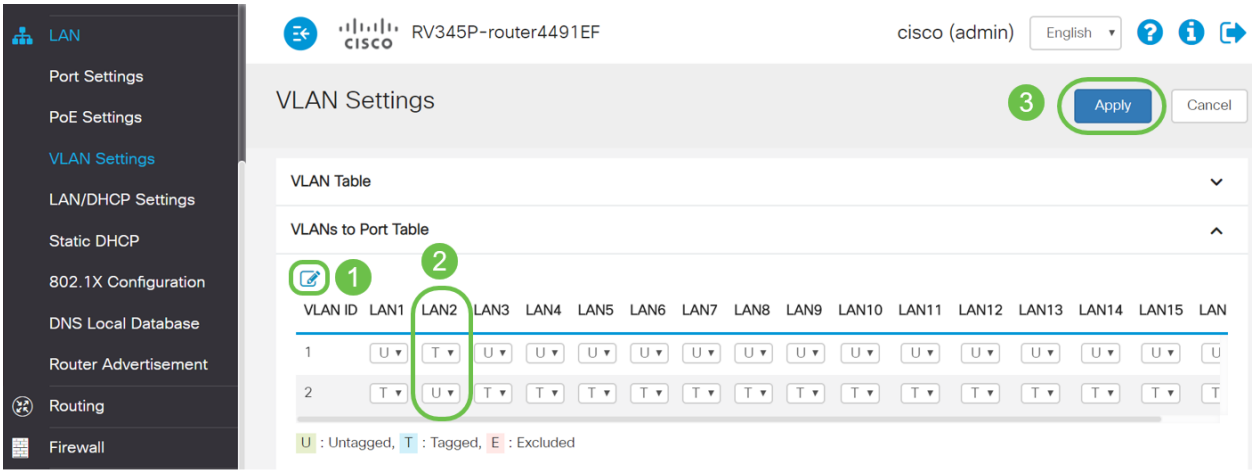
附註：您可以使用IPv6。



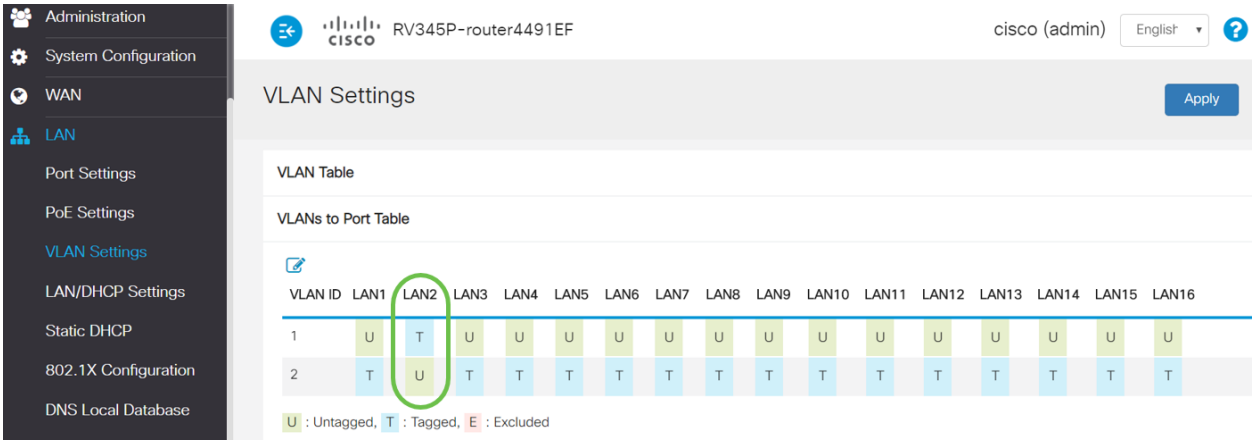
步驟6.導覽至**LAN > VLAN Settings**，並確認VLAN、VLAN1和VLAN2均已啟用*VLAN間路由*。此組態將啟用兩個VLAN之間的通訊。按一下「**Apply**」。



步驟7.要在*LAN2埠上為*VLAN2分配未標籤的流量，請按一下*VLAN to Port Table選項下的edit*按鈕。現在，在LAN2連線埠下，從下拉選單中選擇*VLAN1*的**T**（標籤）選項，以及VLAN2*的***U**（未標籤）選項。按一下「**Apply**」以儲存組態。此組態會轉送LAN2連線埠上VLAN2的未標籤流量，如此一來PC網路介面卡(NIC)（通常無法進行VLAN標籤）便可以從VLAN2取得DHCP IP，並成為VLAN2的一部分。

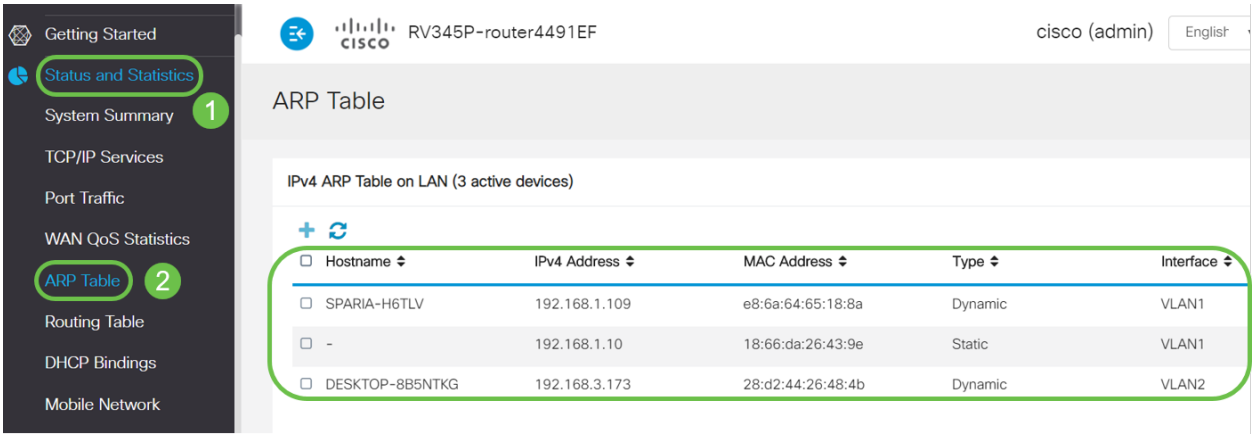


步驟8.檢驗*LAN2*埠的VLAN*2設*置是否顯示為U*（未標籤）*。 對於其餘的LAN埠，VLAN2設定*將為T(標籤)*,VLAN1流量將為*U（未標籤）*。

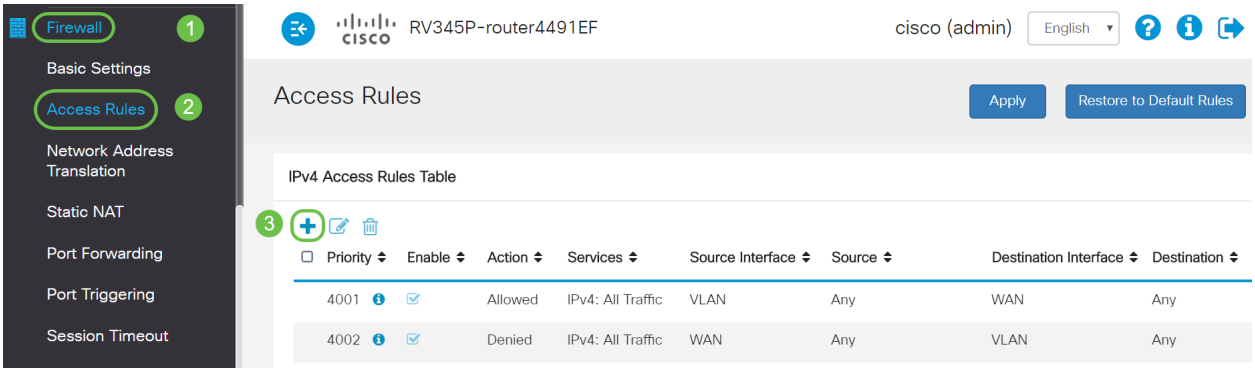


步驟9.導覽至**Status and Statistics > ARP Table**，然後確認PC的動態*IPv4*位址位於不同的VLAN中。

附註：VLAN1上的伺服器IP已靜態分配。



步驟10.應用ACL以限制伺服器(IPv4:192.168.1.10/24)VLAN2使用者訪問。要配置ACL，請導航到**Firewall > Access Rules**，然後點選**plus**圖示新增新規則。



步驟11.配置訪*問規則*引數。在此方案中，引數如下：

規則狀態：啟用

Action:拒絕

服務：所有流量

日誌：正確

源介面：VLAN2

來源位址:任何

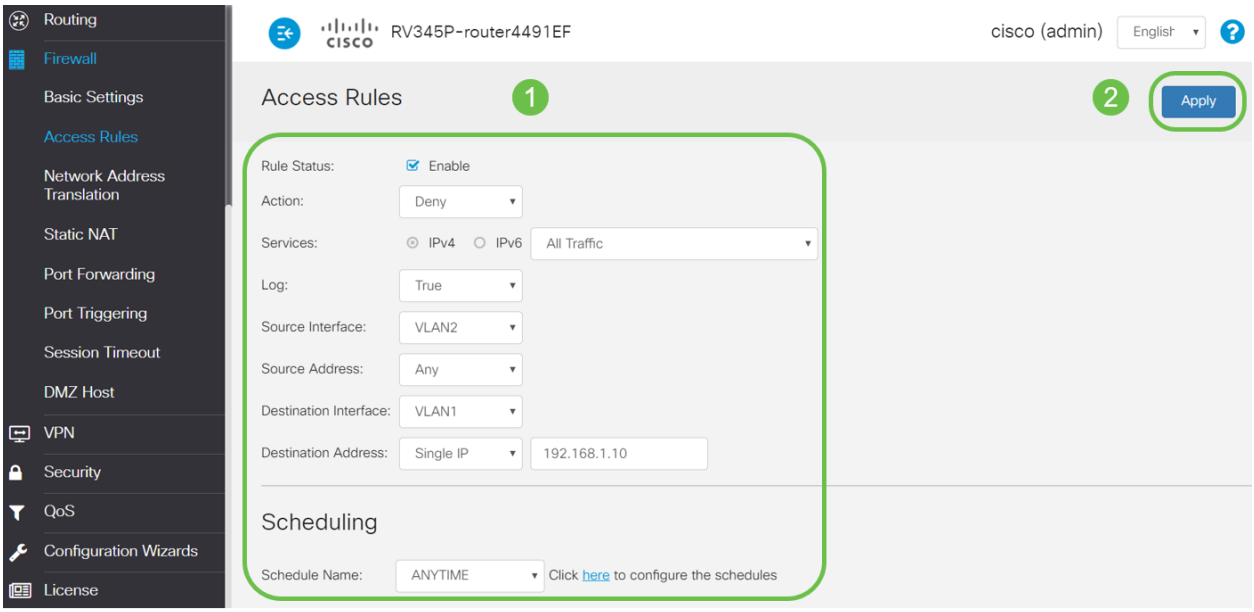
目標介面：VLAN1

目的地位址:單個IP 192.168.1.10

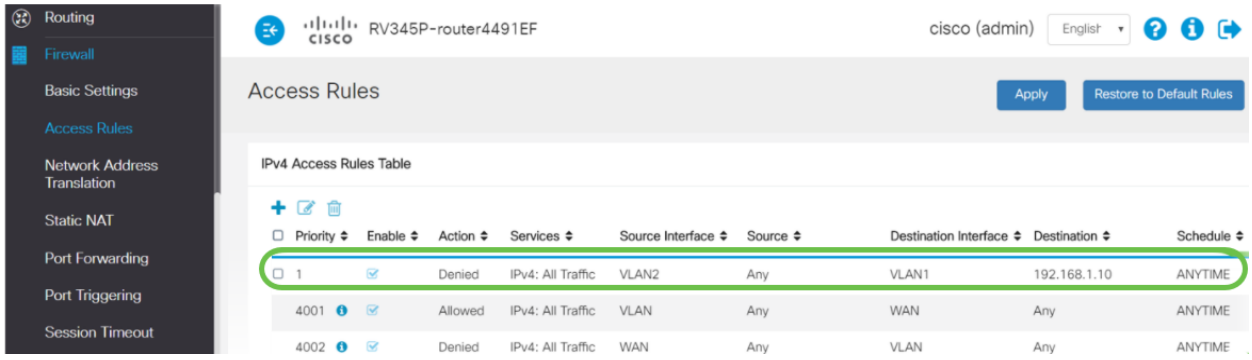
計畫名稱：隨時隨地

按一下「**Apply**」。

附註：在本例中，我們拒絕從VLAN2訪問伺服器的任何裝置，然後允許訪問VLAN1中的其他裝置。您的需求可能會有所不同。



步驟12. *Access Rules*清單將顯示如下：



訪問規則被明確定義為限制伺服器192.168.1.10對VLAN2使用者的訪問。

驗證

要驗證服務，請開啟命令提示符。在Windows平台上，可通過按一下Windows按鈕，然後在電腦左下方的搜尋框中鍵入**cmd**，然後從選單中選擇**Command Prompt**來實現。

輸入以下命令：

- 在VLAN2中的PC(192.168.3.173)上，對伺服器(IP:192.168.1.10）。 您將收到*Request timed out*通知，這意味著不允許通訊。
- 在VLAN2中的PC(192.168.3.173)上，對VLAN1中的其他PC(192.168.1.109)執行ping操作。您將收到成功的回覆。

```
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
```

結論

您已看到在RV34x系列路由器上配置VLAN間路由的必要步驟以及如何執行目標ACL限制。現在，您可以利用所有這些知識，在網路中建立符合需求的VLAN!