Inter-VLAN-routing op een RV34x-router met gerichte ACL-beperkingen

Doel

Dit artikel legt uit hoe u Inter-Virtual Local Area Network (VLAN) routing op een RV34x Series router met gerichte toegangscontrolelijst (ACL) kunt configureren om bepaalde verkeer te beperken. Het verkeer kan worden beperkt door IP-adres, een adresgroep of een protocoltype.

Inleiding

VLAN's zijn groot, zij definiëren uitzenddomeinen in een Layer 2 netwerk. Broadcast-domeinen worden normaal gesproken begrensd door routers omdat routers geen uitzendframes doorsturen. Layer 2-switches maken broadcast-domeinen gebaseerd op de configuratie van de switch. Het verkeer kan niet direct aan een ander VLAN (tussen uitzending domeinen) binnen de switch of tussen twee switches overgaan. VLAN's geven u de mogelijkheid om verschillende afdelingen onafhankelijk van elkaar te houden. Je zou bijvoorbeeld niet willen dat de verkoopafdeling iets met de boekhoudafdeling te maken heeft.

Onafhankelijkheid is fantastisch, maar wat als je wilt dat de eindgebruikers in de VLAN's elkaar kunnen leiden? Het kan nodig zijn dat de verkoopafdeling de boekhouding of de timesheets bij de boekhoudafdeling indient. De boekhoudafdeling zou de verkoopploeg op de hoogte willen stellen van hun loon- of verkoopnummer. Dat is wanneer de routing tussen VLAN’s de dag opslaat!

Voor communicatie tussen VLAN’s is een OSI-laag (Open Systems Interconnecties) op laag 3 nodig, meestal een router. Dit Layer 3 apparaat moet een IP-adres (Internet Protocol) in elke VLAN-interface hebben en een aangesloten route naar elk van deze IP-subnetten hebben. De gastheren in elk IP kunnen dan worden gevormd om de respectieve IP van de interface van VLAN adressen als hun standaardgateway te gebruiken. Wanneer deze ingesteld zijn, kunnen eindgebruikers een bericht naar een eindgebruiker in het andere VLAN versturen. Klinkt perfect, toch?

Maar wacht, hoe zit het met de server in boekhouding? Er is gevoelige informatie op die server die beschermd moet blijven. Geen angst, daar is ook een oplossing voor! Toegangsregels of -beleid op de RV34x Series router staan de configuratie van regels toe om de beveiliging in het netwerk te verhogen. ACL’s zijn lijsten die het verkeer blokkeren of verhinderen dat het van en naar bepaalde gebruikers wordt verzonden. Toegangsregels kunnen zo worden ingesteld dat ze de hele tijd of op basis van vastgestelde schema's van kracht zijn.

Dit artikel zal u door de stappen van het configureren van een tweede VLAN, routing tussen VLAN en ACL lopen.

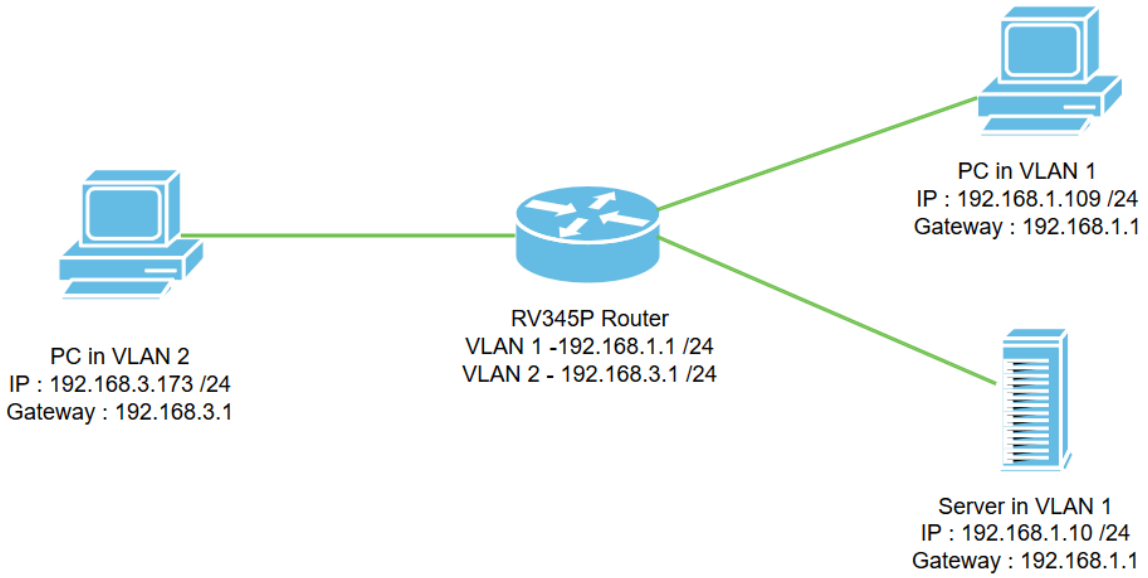
Toepasselijke apparaten

- RV340
- RV340 W
- RV345
- RV345P router

Softwareversie

- 1.0.03.16

Topologie



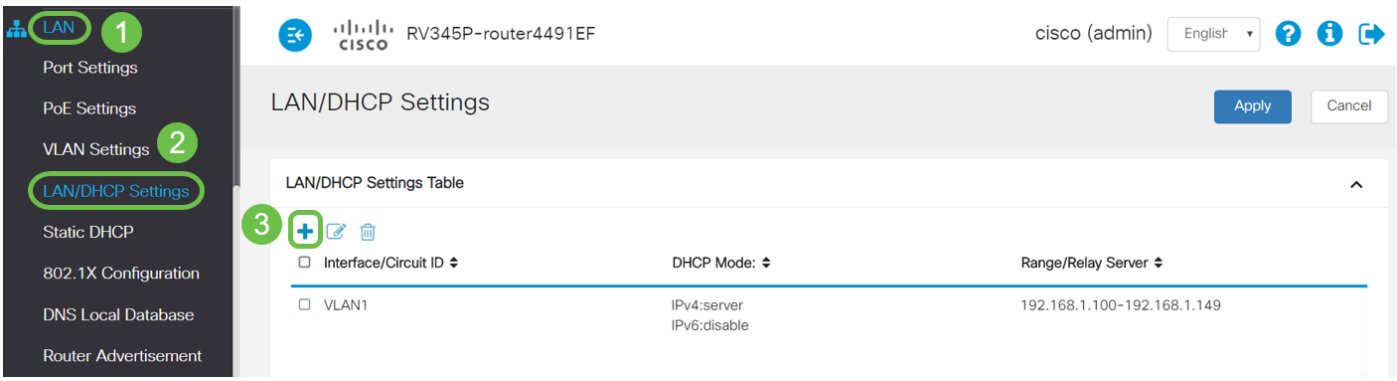
In dit scenario zal de routing tussen VLAN's voor zowel VLAN1 als VLAN2 ingeschakeld zijn zodat de gebruikers in deze VLAN's met elkaar kunnen communiceren. Als veiligheidsmaatregel zullen we voorkomen dat VLAN2-gebruikers toegang hebben tot de VLAN1 server [Internet Protocol versie 4 (IPv4): 192.168.1.10 /24].

Gebruikte routerpoorten:

- De PC (PC) in VLAN1 wordt aangesloten op de *LAN1* poort.
- De PC (PC) in VLAN2 wordt aangesloten op de *LAN2* poort.
- De server in VLAN1 is aangesloten op de *LAN3* poort.

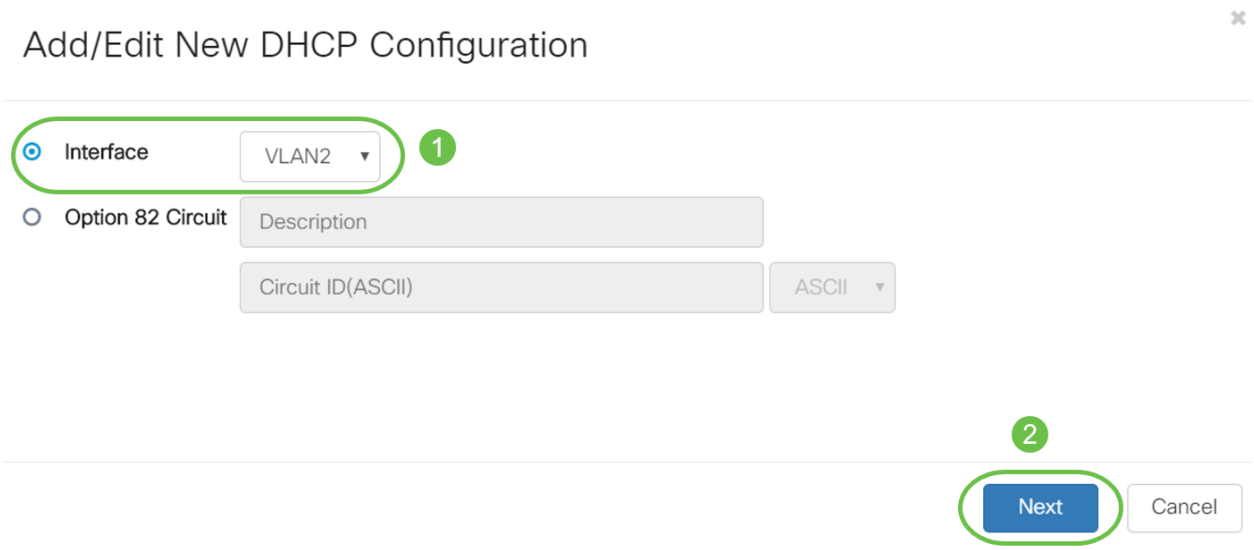
Configuratie

Stap 1. Meld u aan bij het web-configuratie hulpprogramma van de router. Als u een nieuwe VLAN-interface op de router wilt toevoegen, navigeer dan naar **LAN > LAN/DHCP-instellingen** en klik vervolgens op het **pictogram** onder het *tabblad LAN/DHCP-instellingen*.

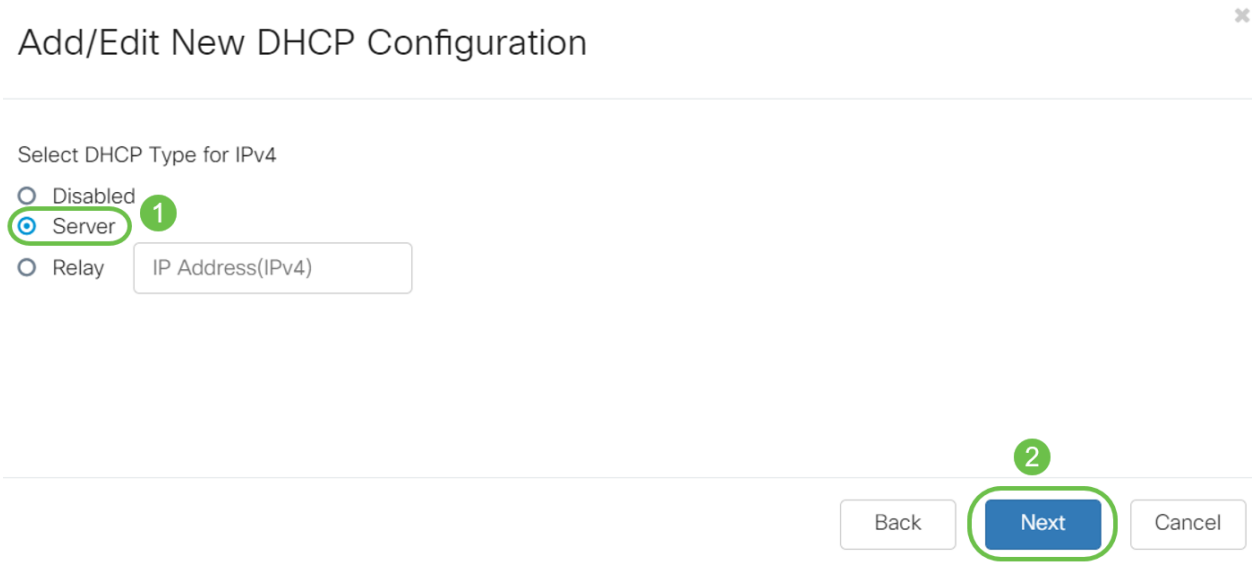


Opmerking: De VLAN1 interface wordt standaard gemaakt op de RV34x-router en de Dynamic Host Configuration Protocol (DHCP) server voor IPv4 is ingeschakeld.

Stap 2. Een nieuw pop-upvenster wordt geopend met *VLAN2* **Interface** geselecteerd, klik op **Volgende**.



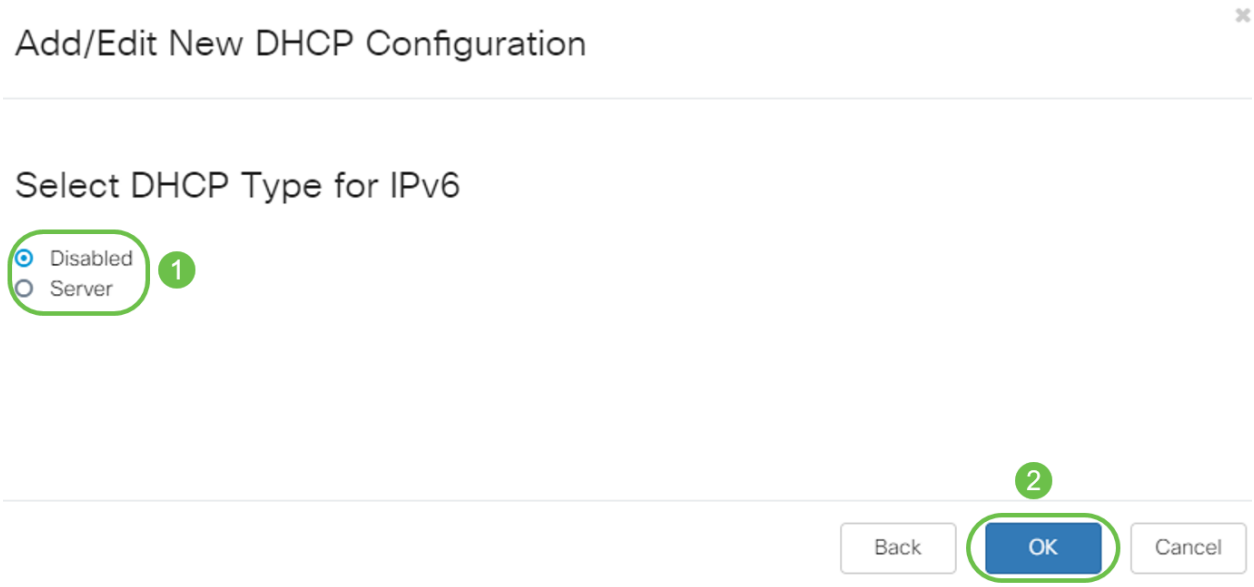
Stap 3. Om de DHCP-server op de VLAN2-interface in te schakelen, *selecteert u DHCP-type voor IPv4* selectieve **server**. Klik op **Volgende**.



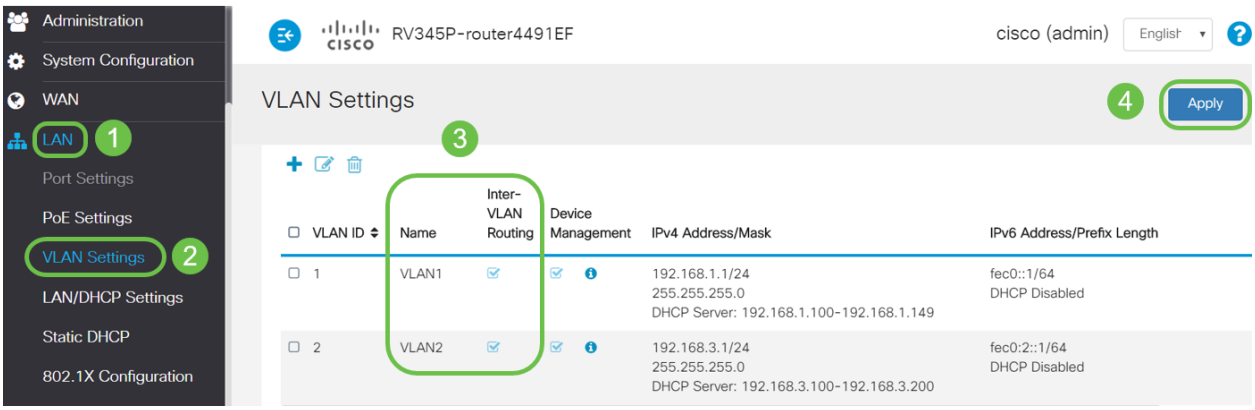
Stap 4. Voer de parameters voor de configuratie van de DHCP-server in, inclusief *Clientstarttijd, bereikstart*, *bereik* en *DNS-server.* Klik op **Volgende**.

Stap 5. (Optioneel) U kunt het *DHCP-type* voor *IPv6* uitschakelen door het aanvinkvakje **Uitgeschakeld** te selecteren omdat dit voorbeeld op IPv4 is gebaseerd. Klik op **OK**. DHCP-serverconfiguratie is voltooid.

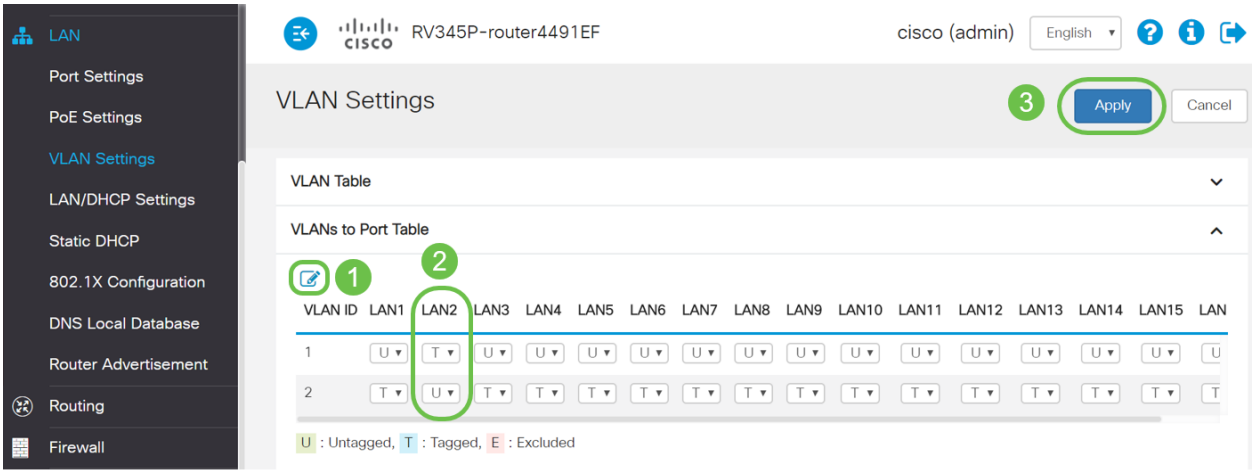
Opmerking: U kunt IPv6 gebruiken.



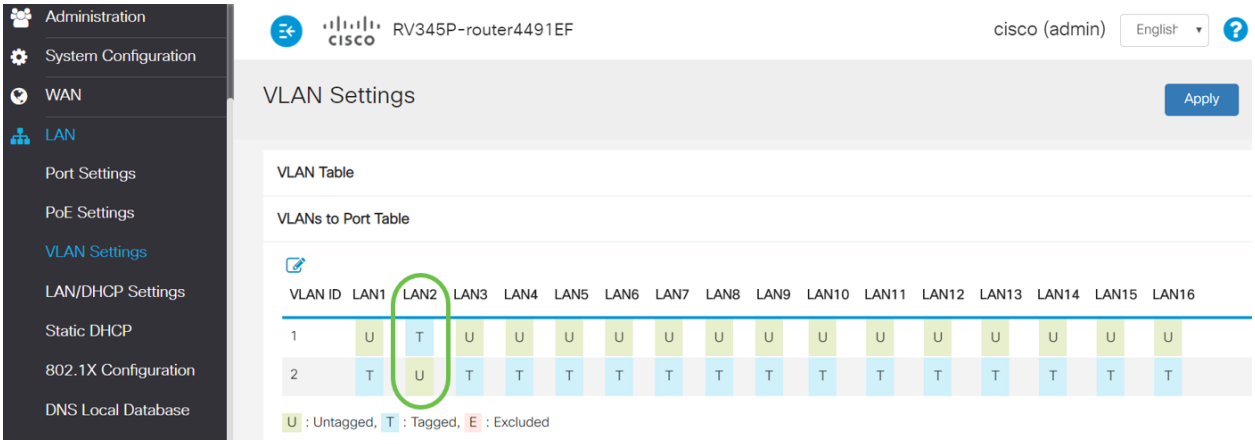
Stap 6. Navigeer naar **LAN > Instellingen van VLAN** en controleer of de *Routing* tussen *VLAN's* zowel voor VLAN's als voor VLAN's is ingeschakeld. Deze configuratie zal de communicatie tussen beide VLAN's vergemakkelijken. Klik op **Toepassen**.



Stap 7. Als u het niet-gelabelde verkeer voor VLAN2 op de *LAN2*-poort wilt toewijzen, klikt u op de knop Bewerken onder de optie *VLAN's in poorttabel*. Selecteer nu onder de *LAN2*-poort de **T** (Tagged) optie voor *VLAN1* en **U** (Untagged) optie voor *VLAN2 in het vervolgkeuzemenu.* Klik op **Toepassen** om de configuratie op te slaan. Deze configuratie zal het niet-gelabelde verkeer voor VLAN2 via de LAN2-poort doorsturen, zodat de PC Network Interface Card (NIC), die normaal niet in staat is om VLAN-tags te taggen, de DHCP IP van VLAN2 kan verkrijgen en deel uitmaakt van VLAN2.

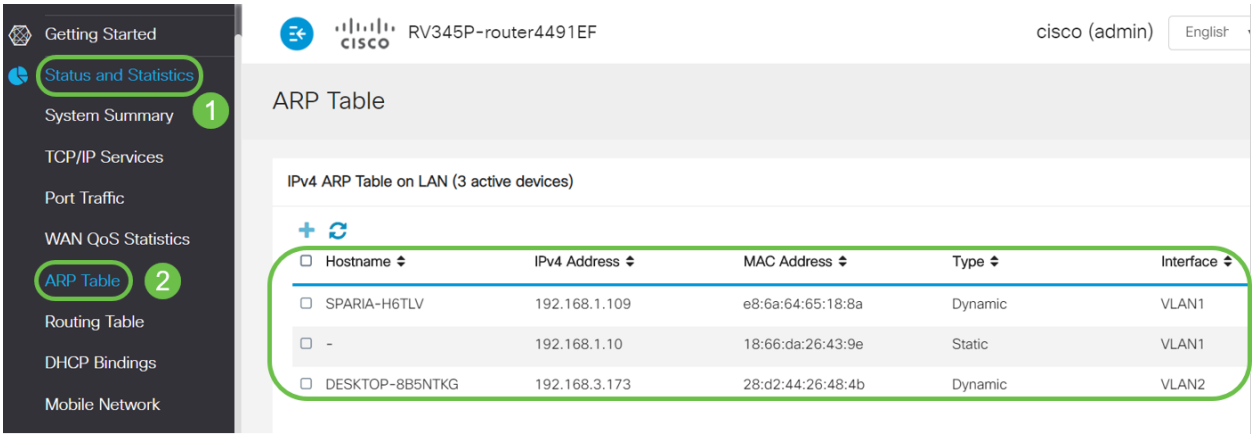


Stap 8. Controleer dat de VLAN2-instellingen voor de *LAN2*-poort worden weergegeven als U *(Untagged)*. Voor de resterende LAN-poorten zullen VLAN2-instellingen *T (Tagged)* en VLAN1-verkeer *U (Untagged)* zijn.

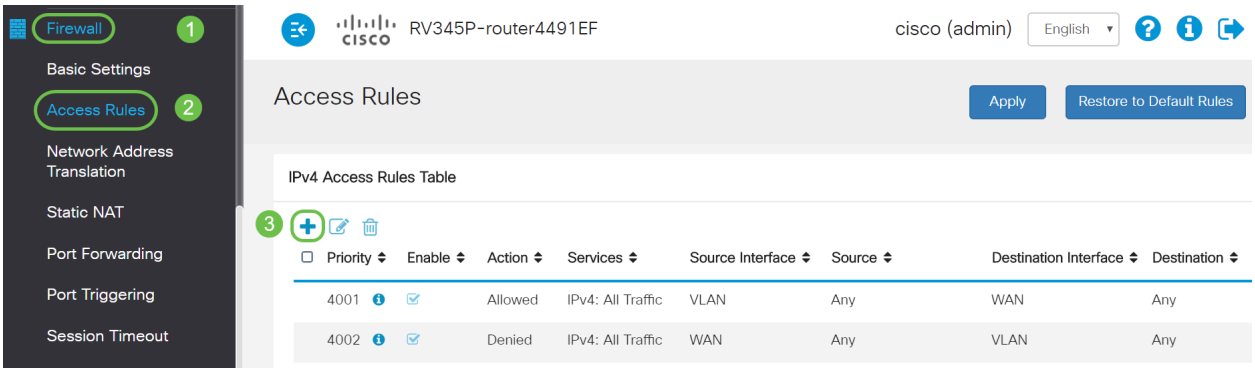


Stap 9. Navigeer naar **Status en Statistieken > ARP Tabel** en controleer het dynamische *IPv4-adres* voor de PC's op verschillende VLAN's.

Opmerking: De server IP op VLAN1 is statistisch toegewezen.



Stap 10. Pas ACL toe om de server (IPv4: 192.168.1.10/24) toegang van VLAN2-gebruikers. Om ACL te configureren navigeer naar **Firewall > Toegangsregels** en klik op het **pictogram plus** om een nieuwe regel toe te voegen.



Stap 1. Configureer de parameters *van de toegangsregels*. Voor dit scenario zijn de parameters als volgt:

Status regel: inschakelen

Actie: ontkennen

Diensten: Alle verkeer

Log: Waar

Broninterface: VLAN2

Bronadres: Alle

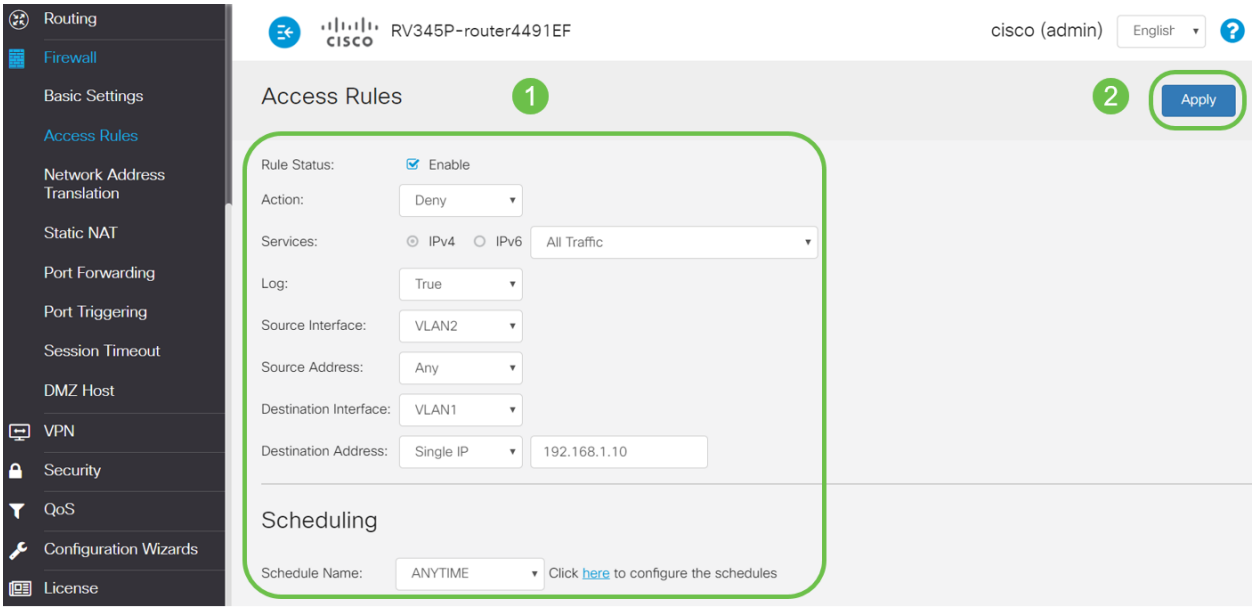
Doelinterface: VLAN1

Doeladres: Enkelvoudige IP-telefoon 192.168.1.10

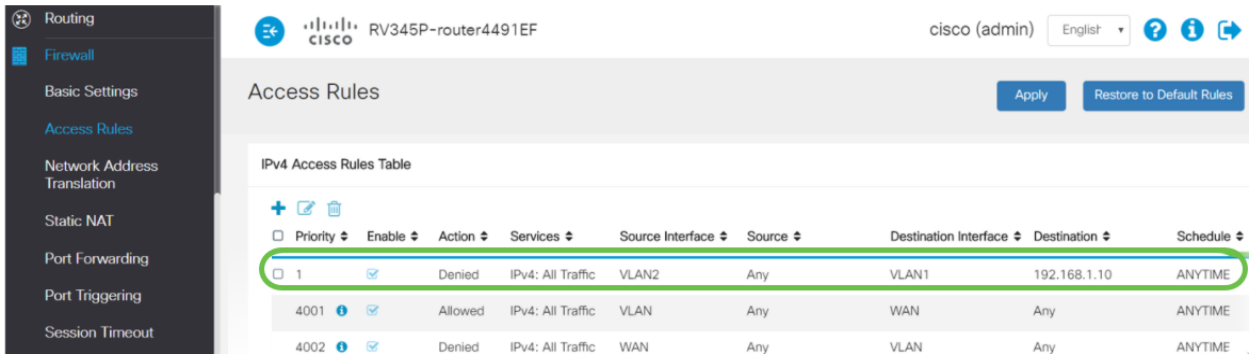
Naam schema: altijd

Klik op **Toepassen**.

Opmerking: In dit voorbeeld ontkenden we toegang van om het even welke apparaten van VLAN2 tot de server, en gaven dan toegang tot de andere apparaten in VLAN1 toe. Uw behoeften kunnen variëren.



Stap 12. De lijst *toegangsregels* toont het volgende:



De toegangsregel is uitdrukkelijk gedefinieerd om de server, 192.168.1.10, toegang van de VLAN2-gebruikers te beperken.

Verificatie

Open de opdrachtmelding om de service te controleren. Op Windows-platforms kan dit worden bereikt door op de knop Windows te klikken en vervolgens **cmd** te typen in het linker onderste

zoekveld van de computer en **Opdrachtsnelheid** in het menu te selecteren.

Geef de volgende opdrachten op:

- Op PC (192.168.3.173) in VLAN2, ping de server (IP: 192.168.1.10). U krijgt een *kennisgeving via* de *tijdelijke versie van het verzoek*, wat betekent dat communicatie niet is toegestaan.
- Op PC (192.168.3.173) in VLAN2, ping de andere PC (192.168.1.109) in VLAN1. U zal een succesvol antwoord krijgen.

```
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
```

Conclusie

U hebt de gewenste stappen gezien om de routing tussen VLAN’s op een RV34x-Series router te configureren en hoe u een gerichte ACL-beperking kunt uitvoeren. Nu kunt u al die kennis gebruiken om VLAN's in uw netwerk te maken die uw behoeften zullen passen!