Inter-VLAN-Routing auf einem RV34x-Router mit Einschränkungen für zielgerichtete Zugriffskontrolllisten

Ziel

In diesem Artikel wird erläutert, wie das VLAN-Routing (Inter-Virtual Local Area Network) auf einem Router der Serie RV34x mit einer Zugriffskontrollliste (ACL) konfiguriert wird, um bestimmten Datenverkehr zu beschränken. Der Datenverkehr kann nach IP-Adresse, Adressengruppe oder Protokolltyp beschränkt werden.

Einführung

VLANs sind hervorragend, sie definieren Broadcast-Domänen in einem Layer-2-Netzwerk. Broadcast-Domänen werden in der Regel durch Router begrenzt, da Router keine Broadcast-Frames weiterleiten. Layer-2-Switches erstellen Broadcast-Domänen basierend auf der Konfiguration des Switches. Der Datenverkehr kann nicht direkt an ein anderes VLAN (zwischen Broadcast-Domänen) innerhalb des Switches oder zwischen zwei Switches weitergeleitet werden. VLANs ermöglichen Ihnen, unterschiedliche Abteilungen voneinander unabhängig zu halten. Sie möchten z. B. nicht, dass sich die Vertriebsabteilung in die Buchhaltung einmischt.

Unabhängigkeit ist fantastisch, aber was ist, wenn die Endbenutzer in den VLANs in der Lage sein sollen, untereinander zu routen? Möglicherweise muss die Verkaufsabteilung der Buchhaltungsabteilung Unterlagen oder Zeitaufzeichnungen vorlegen. Die Buchhaltungsabteilung kann dem Vertriebsteam Benachrichtigungen zu ihren Gehaltsschecks oder Verkaufsnummern senden. Das bedeutet, dass Inter-VLAN-Routing den Tag spart!

Für die VLAN-übergreifende Kommunikation wird ein Layer-3-Gerät (Open Systems Interconnections, in der Regel ein Router) benötigt. Dieses Layer-3-Gerät muss über eine IP-Adresse (Internet Protocol) in jeder VLAN-Schnittstelle verfügen und über eine verbundene Route zu jedem dieser IP-Subnetze verfügen. Die Hosts in jedem IP-Subnetz können dann so konfiguriert werden, dass sie die entsprechenden IP-Adressen der VLAN-Schnittstelle als Standard-Gateway verwenden. Nach der Konfiguration können Endbenutzer eine Nachricht an einen Endbenutzer im anderen VLAN senden. Klingt perfekt, oder?

Aber warte, was ist mit dem Server in Buchhaltung? Es gibt sensible Informationen auf diesem Server, die geschützt bleiben müssen. Haben Sie keine Angst, es gibt auch eine Lösung dafür! Zugriffsregeln oder Richtlinien auf dem Router der Serie RV34x ermöglichen die Konfiguration von Regeln zur Erhöhung der Sicherheit im Netzwerk. ACLs sind Listen, die das Senden von Datenverkehr an und von bestimmten Benutzern blockieren oder zulassen. Zugriffsregeln können so konfiguriert werden, dass sie jederzeit gültig sind oder auf definierten Zeitplänen basieren.

Dieser Artikel führt Sie durch die Schritte zur Konfiguration eines zweiten VLAN, Inter-VLAN-Routing und einer ACL.

Anwendbare Geräte

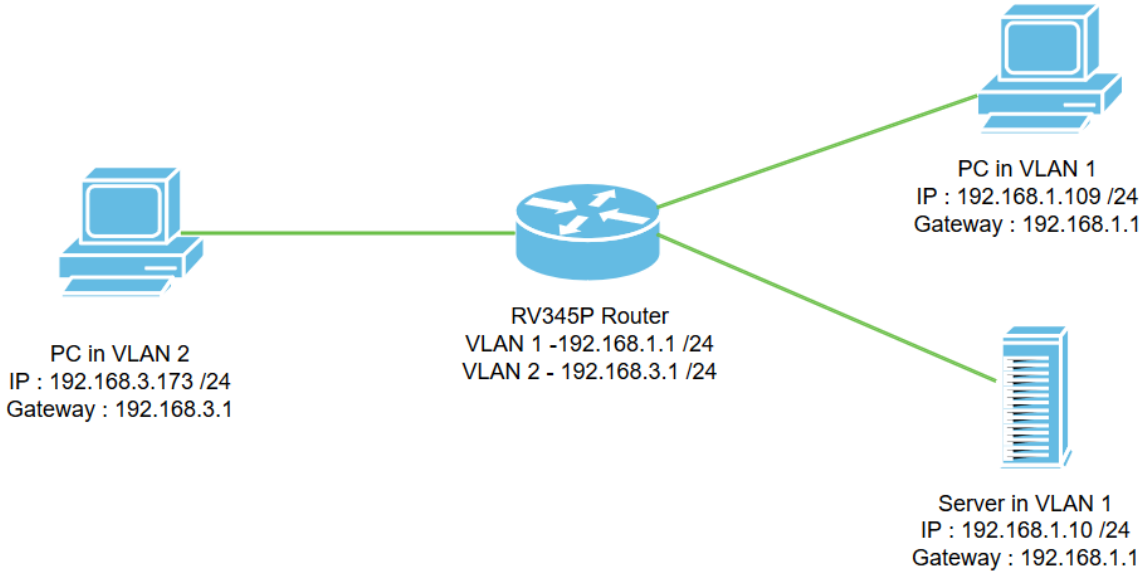
- RV340
- RV340 W

- RV345
- RV345P

Softwareversion

- 1,0,03,16

Topologie



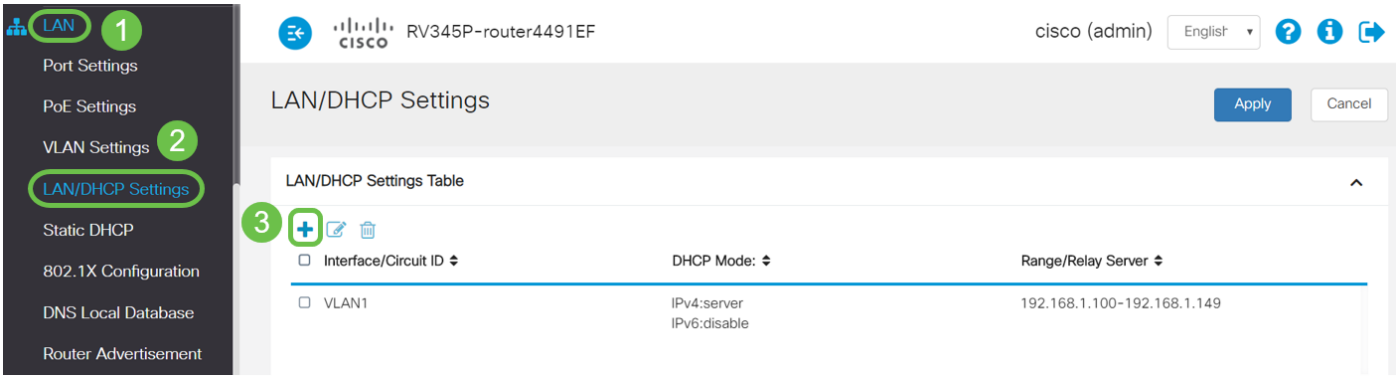
In diesem Szenario wird VLAN-übergreifendes Routing sowohl für VLAN1 als auch für VLAN2 aktiviert, sodass die Benutzer in diesen VLANs miteinander kommunizieren können. Als Sicherheitsmaßnahme verhindern wir, dass VLAN2-Benutzer auf den VLAN1-Server zugreifen können [Internet Protocol Version 4 (IPv4): 192.168.1.10/24].

Verwendete Router-Ports:

- Der Computer (PC) in VLAN1 ist an den *LAN1*-Port angeschlossen.
- Der Computer (PC) in VLAN2 ist über den *LAN2*-Port verbunden.
- Der Server in VLAN1 ist über den *LAN3*-Port verbunden.

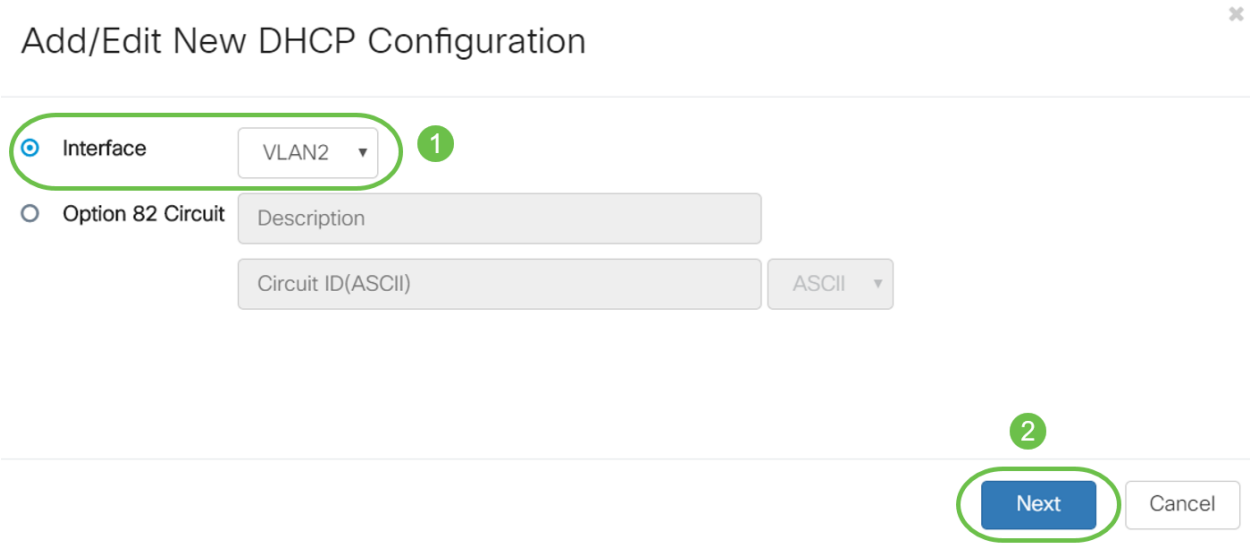
Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurations-Dienstprogramm des Routers an. Um dem Router eine neue VLAN-Schnittstelle hinzuzufügen, navigieren Sie zu **LAN > LAN/DHCP Settings** und klicken Sie auf das **Pluszeichen** unter der *Tabelle für LAN/DHCP-Einstellungen*.



Hinweis: Die VLAN1-Schnittstelle wird standardmäßig auf dem RV34x-Router erstellt, und der Dynamic Host Configuration Protocol (DHCP)-Server für IPv4 ist in diesem Fall aktiviert.

Schritt 2: Ein neues Popup-Fenster wird geöffnet, in dem *VLAN2*-**Schnittstelle** ausgewählt ist. Klicken Sie auf **Weiter**.

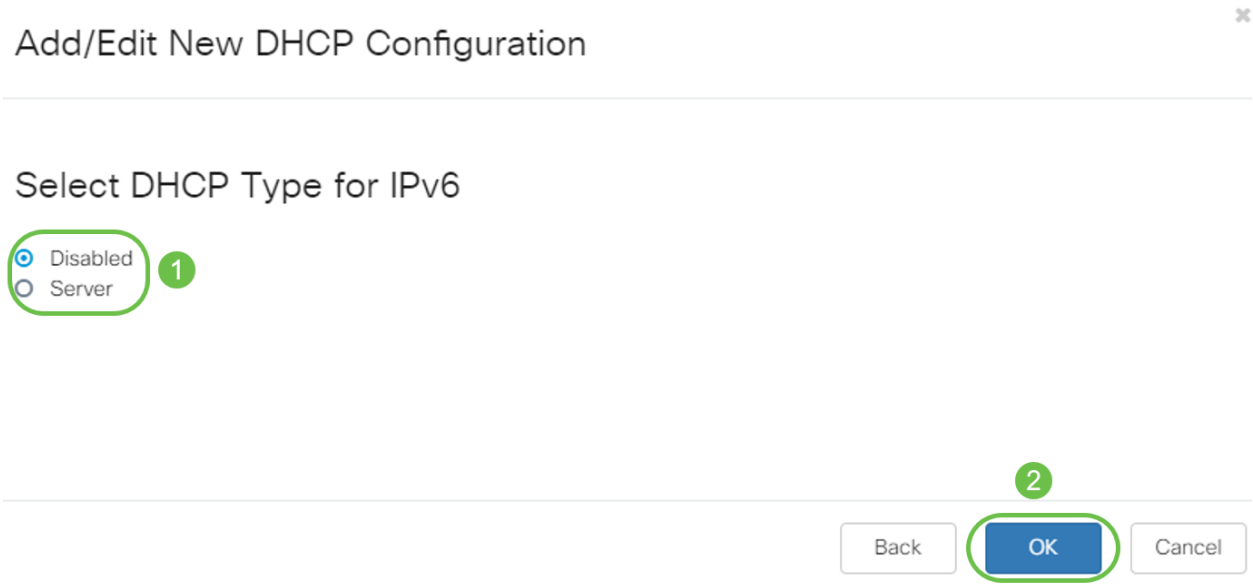


Schritt 3: Um den DHCP-Server auf der VLAN2-Schnittstelle zu aktivieren, wählen Sie unter *DHCP Type for IPv4 (DHCP-Typ für IPv4 auswählen)* **Server** aus. Klicken Sie auf **Weiter**.

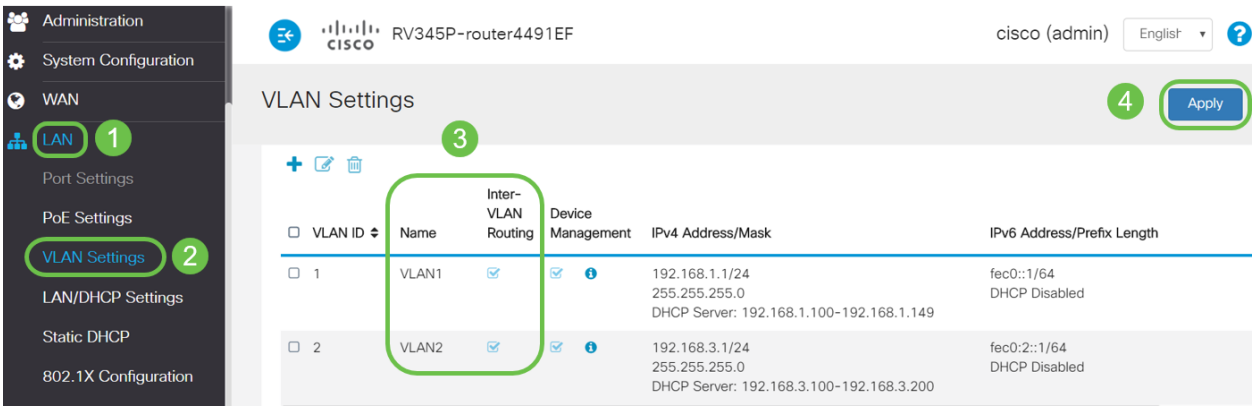
Schritt 4: Geben Sie die Konfigurationsparameter für den DHCP-Server ein, z. B. *Client Lease Time, Range Start*, Range End und *DNS Server.* Klicken Sie auf **Weiter**.

Schritt 5: (Optional) Sie können den *DHCP-Typ für IPv6* deaktivieren, indem Sie das **Kontrollkästchen Deaktiviert** aktivieren, da dieses Beispiel auf IPv4 basiert. Klicken Sie auf **OK**. Die DHCP-Serverkonfiguration ist abgeschlossen.

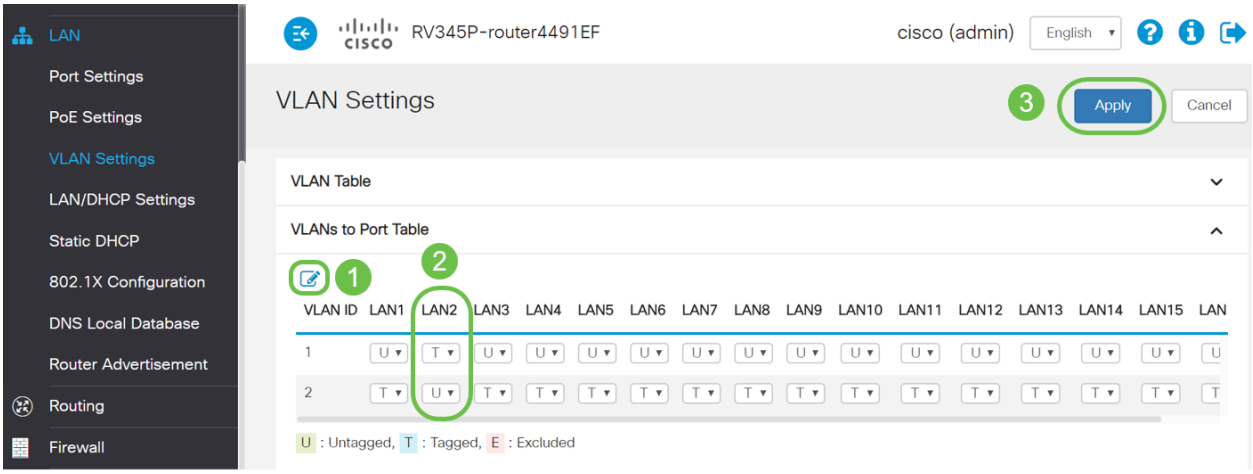
Hinweis: Sie können IPv6 verwenden.



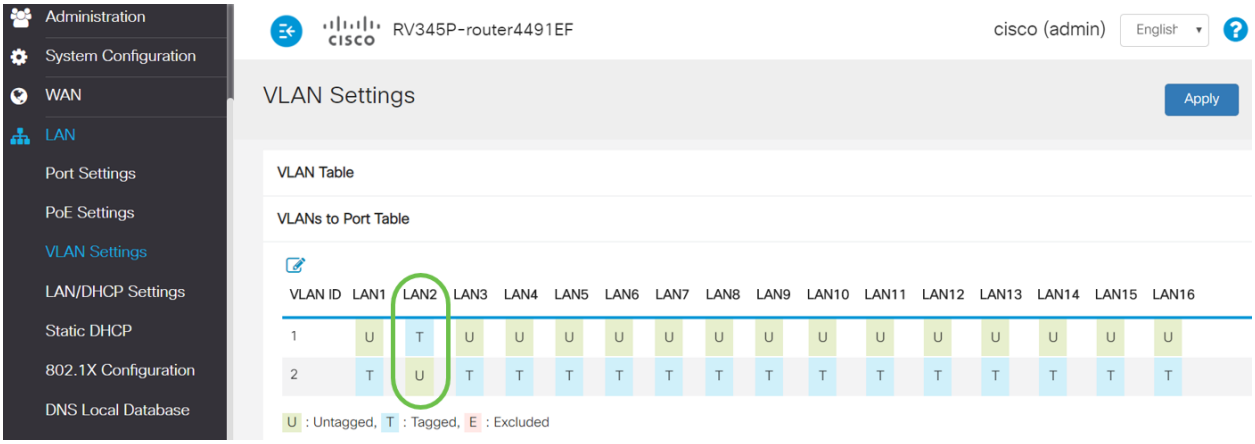
Schritt 6: Navigieren Sie zu **LAN > VLAN Settings**, und überprüfen Sie, ob das *VLAN-übergreifende Routing* für die VLANs VLAN1 und VLAN2 aktiviert ist. Diese Konfiguration ermöglicht die Kommunikation zwischen den beiden VLANs. Klicken Sie auf **Übernehmen**.



Schritt 7: Um den nicht gekennzeichneten Datenverkehr für VLAN2 am *LAN2*-Port zuzuweisen, klicken Sie unter der Option "*VLANs to Port Table" auf die Schaltfläche "*Bearbeiten". Wählen Sie jetzt unter dem *LAN2*-Port die **T** (Tagged)-Option für *VLAN1* und **U** (Untagged) für *VLAN2 aus dem Dropdown-Menü aus.* Klicken Sie auf **Apply**, um die Konfiguration zu speichern. Diese Konfiguration leitet den nicht getaggten Datenverkehr für VLAN2 an den LAN2-Port weiter, sodass die PC-Netzwerkkarte (NIC), die normalerweise nicht VLAN-Tagging unterstützen kann, die DHCP-IP von VLAN2 abrufen kann und Teil von VLAN2 ist.

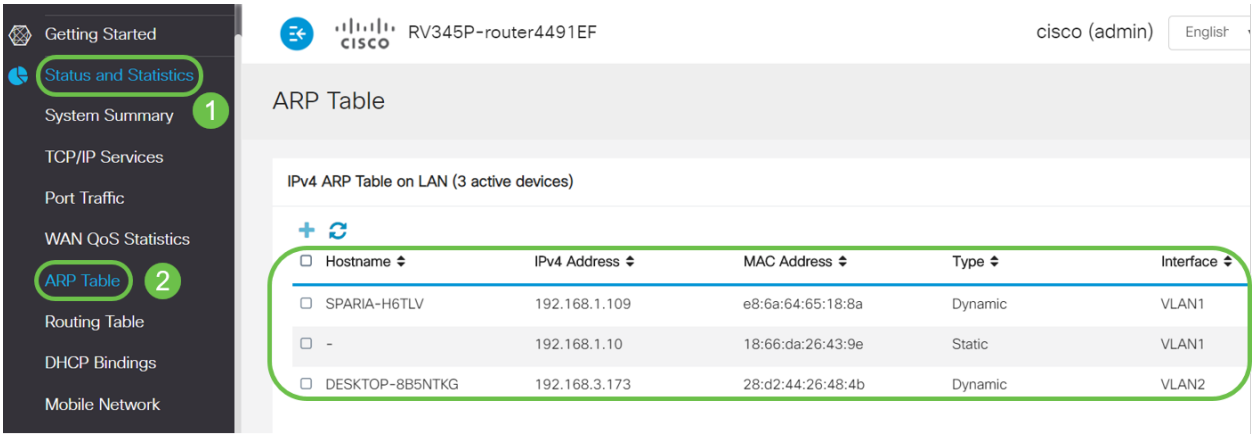


Schritt 8: Überprüfen Sie, ob die VLAN2-Einstellungen für den *LAN2*-Port als U *(Untagged)* angezeigt werden. Für die verbleibenden LAN-Ports sind die VLAN2-Einstellungen *T (Tagged)* und der VLAN1-Datenverkehr *U (Untagged)*.

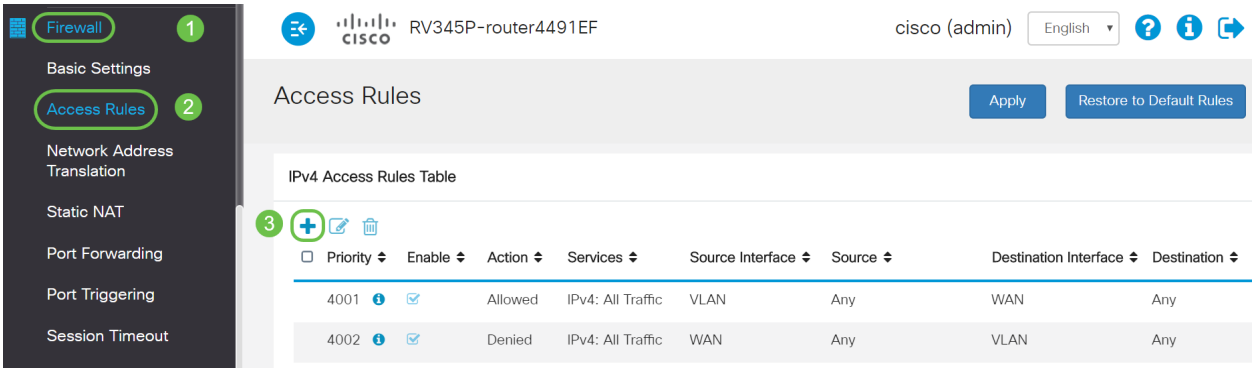


Schritt 9: Navigieren Sie zu **Status und Statistik > ARP Table**, und überprüfen Sie, ob sich die dynamische *IPv4-Adresse* der PCs in unterschiedlichen VLANs befindet.

Hinweis: Die Server-IP in VLAN1 wurde statisch zugewiesen.



Schritt 10: ACL anwenden, um den Server einzuschränken (IPv4: 192.168.1.10/24) Zugriff von VLAN2-Benutzern. Um die ACL zu konfigurieren, navigieren Sie zu **Firewall > Access Rules** (Firewall > Zugriffsregeln), und klicken Sie auf das **Pluszeichen**, um eine neue Regel hinzuzufügen.



Schritt 11: Konfigurieren Sie die Parameter *für Zugriffsregeln*. Für dieses Szenario sind folgende Parameter erforderlich:

Regelstatus: Aktivieren

Aktion: Ablehnen

Services: Gesamter Datenverkehr

Protokoll: Richtig

Quellschnittstelle: VLAN2

Quelladresse: Beliebig

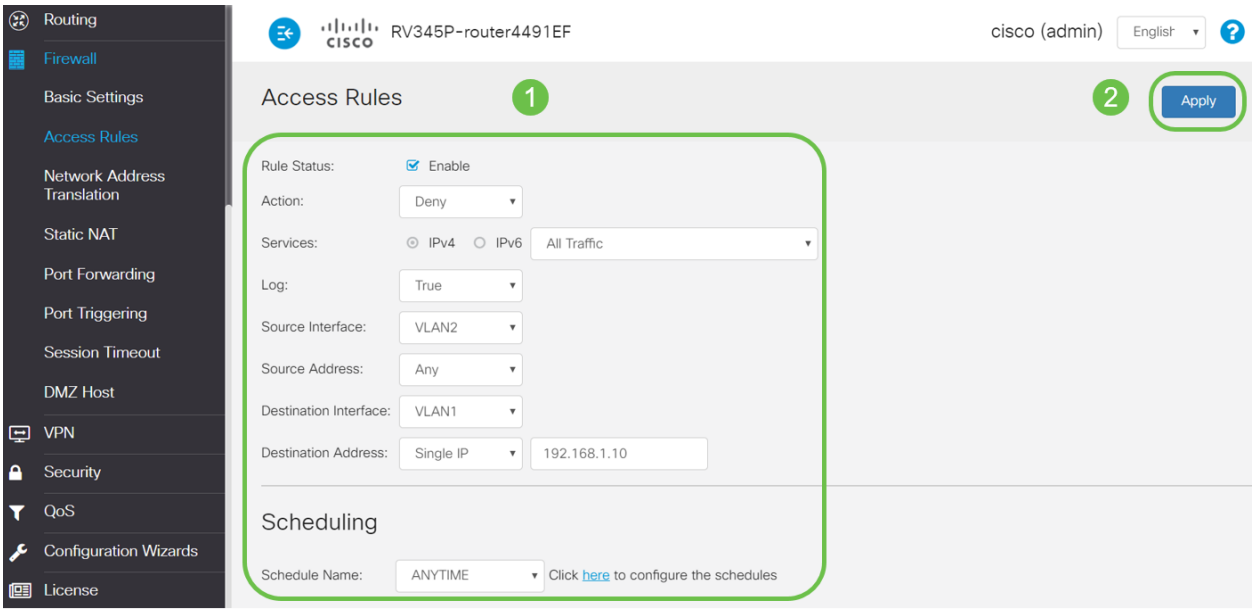
Zielschnittstelle: VLAN1

Zieladresse: Eine IP-Adresse 192.168.1.10

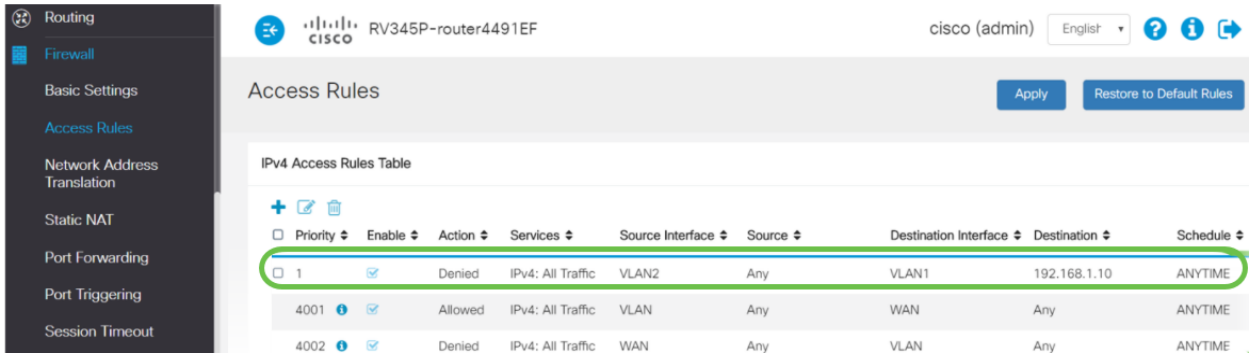
Name des Zeitplans: Jederzeit

Klicken Sie auf **Übernehmen**.

Hinweis: In diesem Beispiel haben wir den Zugriff aller Geräte von VLAN2 auf den Server verweigert und dann den Zugriff auf die anderen Geräte in VLAN1 zugelassen. Ihre Anforderungen können variieren.



Schritt 12: Die Liste der *Zugriffsregeln* wird wie folgt angezeigt:



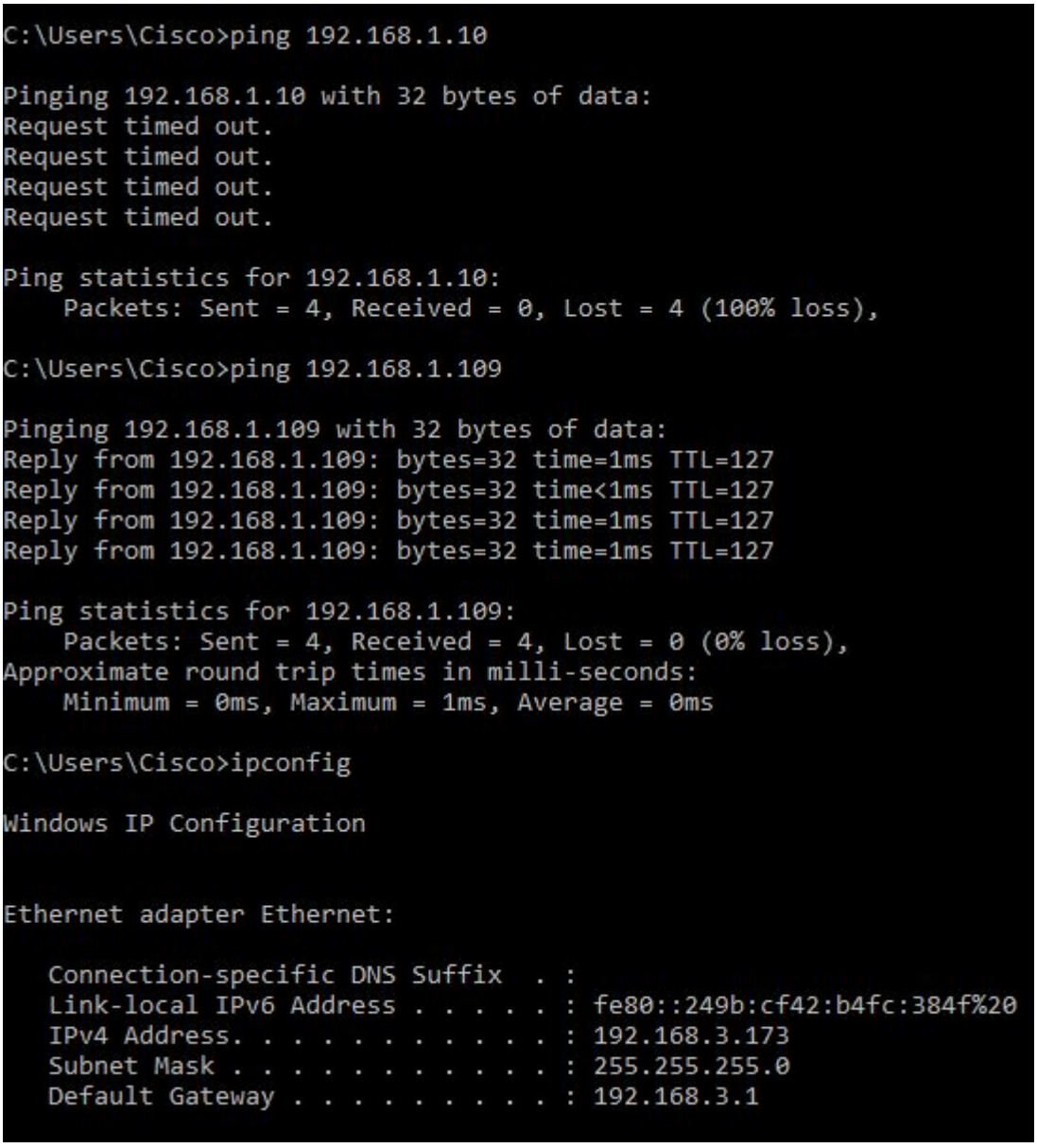
Die Zugriffsregel ist explizit definiert, um den Zugriff des Servers 192.168.1.10 von den VLAN2-Benutzern zu beschränken.

Überprüfung

Öffnen Sie zum Überprüfen des Dienstes die Eingabeaufforderung. Auf Windows-Plattformen kann dies erreicht werden, indem Sie auf die Windows-Schaltfläche klicken und anschließend **cmd** im unteren linken Suchfeld des Computers eingeben und im Menü die **Eingabeaufforderung** auswählen.

Geben Sie die folgenden Befehle ein:

- Pingen Sie auf dem PC (192.168.3.173) in VLAN2 den Server (IP: 192.168.1.10). Sie erhalten eine *Timeout*-Benachrichtigung für *Anfragen*, was bedeutet, dass eine Kommunikation nicht zulässig ist.
- Pingen Sie auf PC (192.168.3.173) in VLAN2 den anderen PC (192.168.1.109) in VLAN1. Sie erhalten eine erfolgreiche Antwort.



Schlussfolgerung

Sie haben die erforderlichen Schritte zur Konfiguration des VLAN-übergreifenden Routings auf einem Router der Serie RV34x und zur Vorgehensweise bei einer Einschränkung der Zugriffskontrollliste gesehen. Sie können dieses Wissen jetzt nutzen, um VLANs in Ihrem Netzwerk zu erstellen, die Ihren Anforderungen entsprechen!