

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.

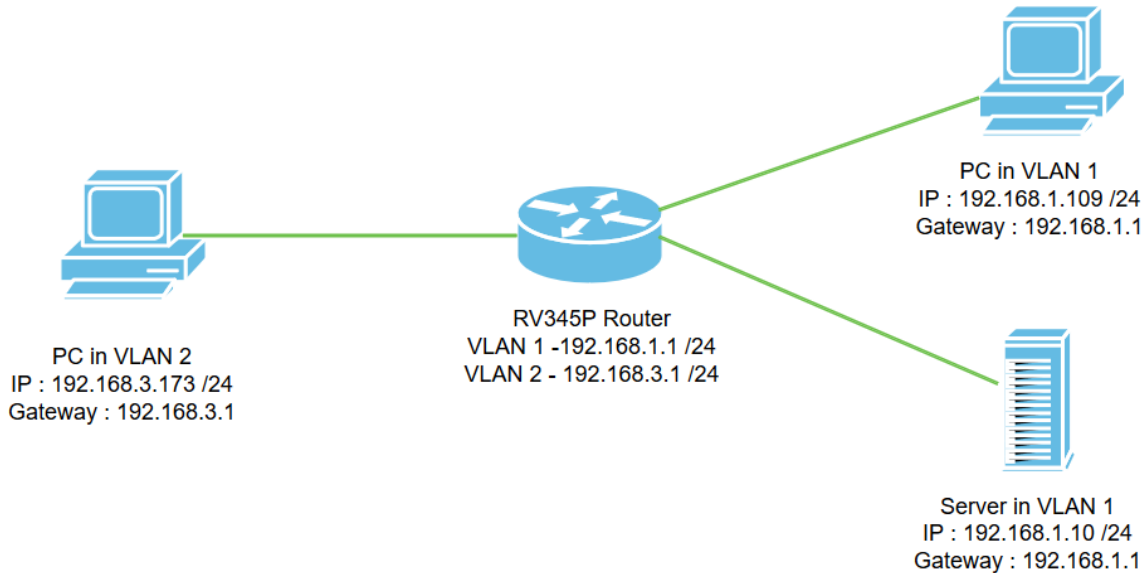
Toepasselijke apparaten

- 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*.

The screenshot shows the Cisco RV345P router web configuration interface. The left sidebar shows the navigation menu with 'LAN/DHCP Settings' selected. The main content area displays the 'LAN/DHCP Settings Table' with the following configuration:

Interface/Circuit ID	DHCP Mode	Range/Relay Server
VLAN1	IPv4:server IPv6:disable	192.168.1.100-192.168.1.149

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**.

Add/Edit New DHCP Configuration ✕

Interface 1

Option 82 Circuit

2

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

Add/Edit New DHCP Configuration ✕

Select DHCP Type for IPv4

Disabled

Server 1

Relay

2

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

Select DHCP Server for IPv4

Client Lease Time: min. (Range: 5-43200, Default: 1440)

Range Start:

Range End:

DNS Server:

Static DNS1:

Static DNS2:

WINS Server:

Network Booting: Enable

1

DHCP Options

Option 66 - IP Address or Host Name of a single TFTP Server:

Option 150 - Comma-separated list of TFTP Server Addresses:

Option 67 - Configuration Filename:

Option 43 - Vendor Specific Information:

2

Back Cancel

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.

Add/Edit New DHCP Configuration



Select DHCP Type for IPv6

Disabled **1**
 Server

2
Back **OK** Cancel

Step 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**.

Administration
System Configuration
WAN
LAN **1**
Port Settings
PoE Settings
VLAN Settings **2**
LAN/DHCP Settings
Static DHCP
802.1X Configuration

RV345P-router4491EF cisco (admin) English ?

VLAN Settings

3

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149	fec0::1/64 DHCP Disabled
2	VLAN2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1/24 255.255.255.0 DHCP Server: 192.168.3.100-192.168.3.200	fec0:2::1/64 DHCP Disabled

4 Apply

Step 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*.

LAN
Port Settings
PoE Settings
VLAN Settings
LAN/DHCP Settings
Static DHCP
802.1X Configuration
DNS Local Database
Router Advertisement
Routing
Firewall

RV345P-router4491EF cisco (admin) English ? ? ?

VLAN Settings

3 Apply Cancel

VLAN Table

VLANs to Port Table

1 **2**

VLAN ID	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6	LAN7	LAN8	LAN9	LAN10	LAN11	LAN12	LAN13	LAN14	LAN15	LAN
1	U	T	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	T	U	T	T	T	T	T	T	T	T	T	T	T	T	T	T

U : Untagged, T : Tagged, E : Excluded

Step 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.

Administration
System Configuration
WAN
LAN
Port Settings
PoE Settings
VLAN Settings
LAN/DHCP Settings
Static DHCP
802.1X Configuration
DNS Local Database

RV345P-router4491EF cisco (admin) English

VLAN Settings

VLAN Table

VLANs to Port Table

VLAN ID	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6	LAN7	LAN8	LAN9	LAN10	LAN11	LAN12	LAN13	LAN14	LAN15	LAN16
1	U	T	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	T	U	T	T	T	T	T	T	T	T	T	T	T	T	T	T

U : Untagged, T : Tagged, E : Excluded

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.

Getting Started
Status and Statistics
System Summary
TCP/IP Services
Port Traffic
WAN QoS Statistics
ARP Table
Routing Table
DHCP Bindings
Mobile Network

RV345P-router4491EF cisco (admin) English

ARP Table

IPv4 ARP Table on LAN (3 active devices)

Hostname	IPv4 Address	MAC Address	Type	Interface
SPARIA-H6TLV	192.168.1.109	e8:6a:64:65:18:8a	Dynamic	VLAN1
-	192.168.1.10	18:66:da:26:43:9e	Static	VLAN1
DESKTOP-8B5NTKG	192.168.3.173	28:d2:44:26:48:4b	Dynamic	VLAN2

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.

Firewall
Basic Settings
Access Rules
Network Address Translation
Static NAT
Port Forwarding
Port Triggering
Session Timeout

RV345P-router4491EF cisco (admin) English

Access Rules

IPv4 Access Rules Table

Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination
4001	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any
4002	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any

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.

The screenshot shows the configuration page for 'Access Rules' on a Cisco RV345P router. The configuration is as follows:

- Rule Status: Enable
- Action: Deny
- Services: IPv4 IPv6 All Traffic
- Log: True
- Source Interface: VLAN2
- Source Address: Any
- Destination Interface: VLAN1
- Destination Address: Single IP 192.168.1.10
- Schedule Name: ANYTIME

The 'Apply' button is highlighted with a green circle (2).

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

The screenshot shows the 'IPv4 Access Rules Table' with the following data:

Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination	Schedule
1	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	VLAN2	Any	VLAN1	192.168.1.10	ANYTIME
4001	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any	ANYTIME
4002	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any	ANYTIME

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-beperving kunt uitvoeren. Nu kunt u al die kennis gebruiken om VLAN's in uw netwerk te maken die uw behoeften zullen passen!