ACL-beste praktijken op RV34x Series router

Doel

Het doel van dit artikel is om beste praktijken voor het creëren van Toegangscontrolelijsten (ACL's) met uw RV34x Series router te beschrijven.

Toepasselijke apparaten | Versie firmware

- RV340 | 1.0.03.20 (laatste download)
- RV340 W | 1.0.03.20 (laatste download)
- RV345 | 1.0.03.20 (laatste download)
- RV345P router | 1.0.03.20 (laatste download)

Inleiding

Wilt u meer controle over uw netwerk? Wilt u extra stappen nemen om uw netwerk veilig te houden? Als dit zo is, kan een Toegangscontrolelijst (ACL) precies zijn wat u nodig hebt.

Een ACL bestaat uit een of meer ACE's (toegangscontrole) die gezamenlijk het netwerkverkeersprofiel definiëren. Dit profiel kan dan worden verwezen door Cisco-softwarefuncties zoals traffic filtering, prioriteit of aangepaste wachtrij. Elke ACL bevat een actie-element (licentie of ontkenning) en een filterelement op basis van criteria zoals bronadres, doeladres, protocol en protocolspecifieke parameters.

Gebaseerd op de criteria die u hebt ingevoerd, kunt u bepaald verkeer van het binnengaan en/of verlaten van een netwerk controleren. Wanneer een router een pakket ontvangt, zou het het pakket onderzoeken om te bepalen of om het pakket door te sturen of te laten vallen dat op uw toegangslijst is gebaseerd.

Het implementeren van dit veiligheidsniveau is gebaseerd op verschillende gebruiksgevallen waarbij rekening wordt gehouden met specifieke netwerkscenario's en beveiligingsbehoeften.

Het is belangrijk om op te merken dat de router automatisch een toegangslijst kan maken gebaseerd op configuraties op uw router. In dit geval, kunt u toegangslijsten zien die u niet kunt wissen tenzij u de routerconfiguraties wijzigt.

Waarom gebruiken we toegangslijsten

- In de meeste gevallen gebruiken we ACL's om een basisniveau van beveiliging te bieden voor de toegang tot ons netwerk. Als u bijvoorbeeld geen ACL's vormt, zijn standaard alle pakketten die door de router worden verzonden toegestaan aan alle delen van ons netwerk.
- ACL's kunnen één host, bereik van IP-adressen of -netwerken toestaan en een andere

host, bereik van IP-adressen of netwerken verhinderen om hetzelfde gebied (host of netwerk) te bereiken.
- Door ACLs te gebruiken, kunt u besluiten welke types van verkeer u op de routerinterfaces door stuurde of geblokkeerd hebt. U kunt bijvoorbeeld Secure Shell (SSH) File Transfer Protocol (SFTP)-verkeer toestaan en tegelijkertijd alle SIP-verkeer (Session Initiation Protocol) blokkeren.

Wanneer gebruikt u toegangslijsten

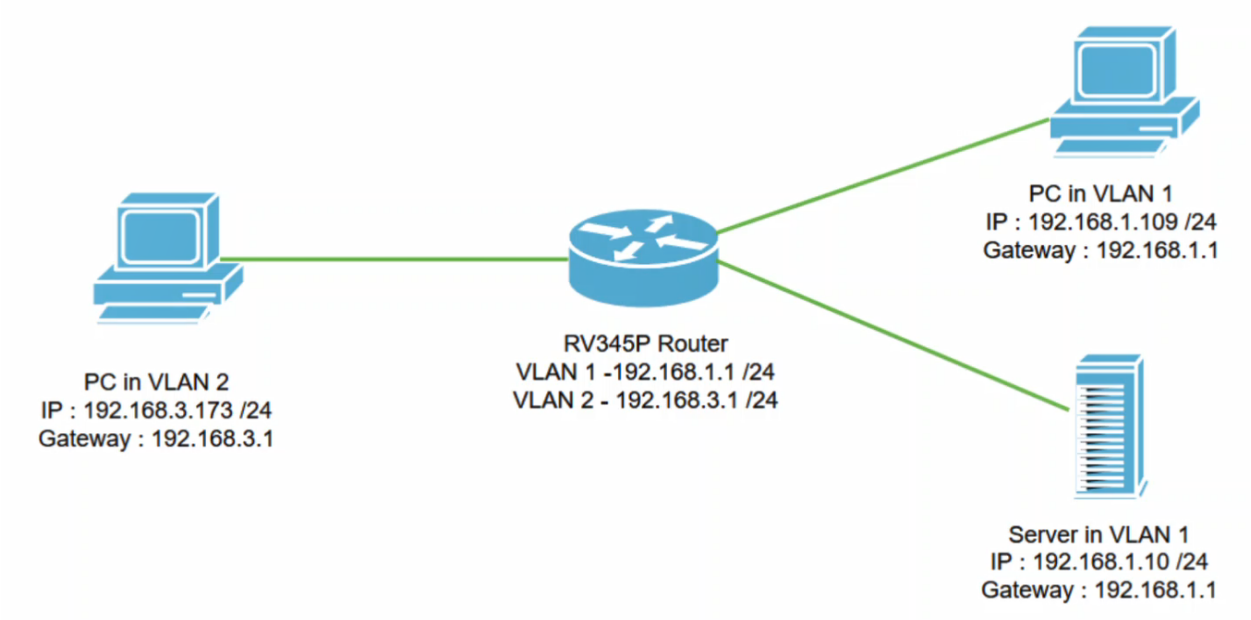
- U dient ACL's in routers te configureren die tussen ons interne netwerk en een extern netwerk worden geplaatst zoals Internet.
- U kunt ACL's gebruiken om verkeer dat een specifiek deel van ons interne netwerk binnenkomt of uitgaat te besturen.
- Wanneer u inkomende of uitgaande verkeer moet filteren, of beide op een interface.
- U dient ACL's per protocol te definiëren om verkeer te controleren.

Beste praktijken voor het configureren van basisbeveiliging met toegangslijsten

- Voer ACL's in die alleen die protocollen, poorten en IP-adressen toestaan die al het andere ontkennen.
- Blokkeer binnenkomende pakketten die de zelfde bestemming en bronadres (landaanval op de router zelf) beweren te hebben.
- Zet blogmogelijkheid op ACL's aan op een interne (vertrouwde) Syslog-host.
- Als u Simple Network Management Protocol (SNMP) op de router gebruikt, moet u SNMP en complexe SNMP-community-string configureren.
- Toestaan alleen interne adressen om de router van de interne interfaces in te voeren en staan alleen verkeer toe dat voor interne adressen is bestemd om de router van de buitenkant (externe interfaces) in te voeren.
- Blokkeer multicast indien niet gebruikt.
- Blokkeer sommige berichttypes van Internet Control Message Protocol (ICMP) (redirect, echo).
- Denk altijd aan de volgorde waarin u de ACL's invoert. Bijvoorbeeld, wanneer de router beslist of om een pakket door te sturen of te blokkeren, test het het pakket tegen elke verklaring in de volgorde waarin ACLs werd gecreëerd.

Implementatie van toegangslijst in Cisco RV34x Series routers

Netwerktopologie voorbeeld



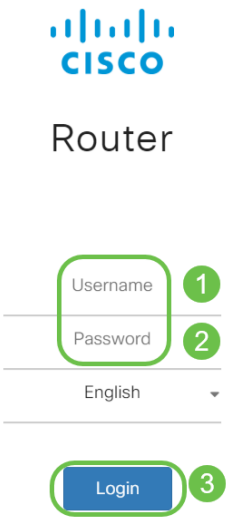
Bijvoorbeeld scenario

In dit scenario zullen we dit netwerkdiagram reproduceren, waar we een RV345P router en twee verschillende VLAN interfaces hebben. We hebben een PC in VLAN 1 en in VLAN2, en we hebben ook een server in VLAN 1. De routing tussen VLAN's is geactiveerd, dus VLAN 1 en VLAN 2 gebruikers kunnen met elkaar communiceren. Nu gaan we de toegangsregel toepassen om de communicatie tussen de VLAN 2 gebruiker naar deze server in VLAN 1 te beperken.

Configuratie voorbeeld

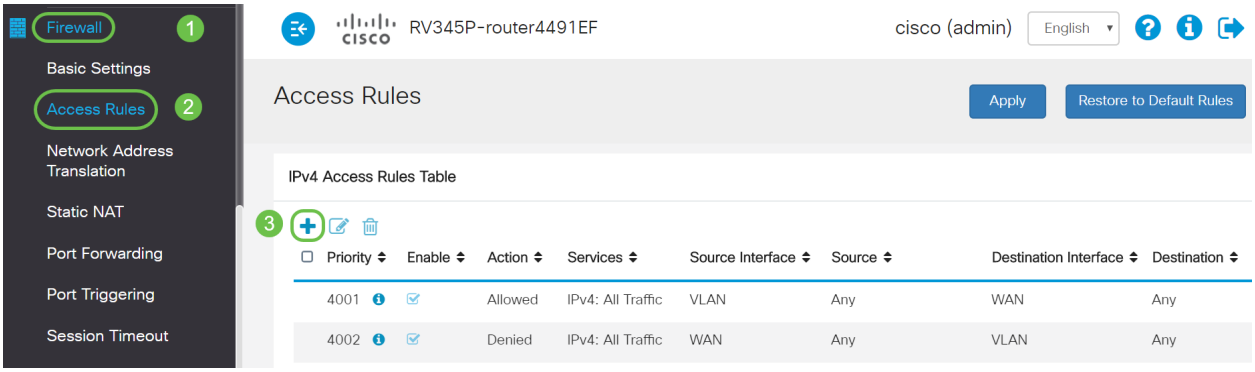
Stap 1

Meld u aan bij het Web User Interface (UI) van de router met behulp van de aanmeldingsgegevens die u hebt ingesteld.



Stap 2

Om ACL te configureren navigeer naar **Firewall > Toegangsregels** en klik op het **pictogram plus** om een nieuwe regel toe te voegen.



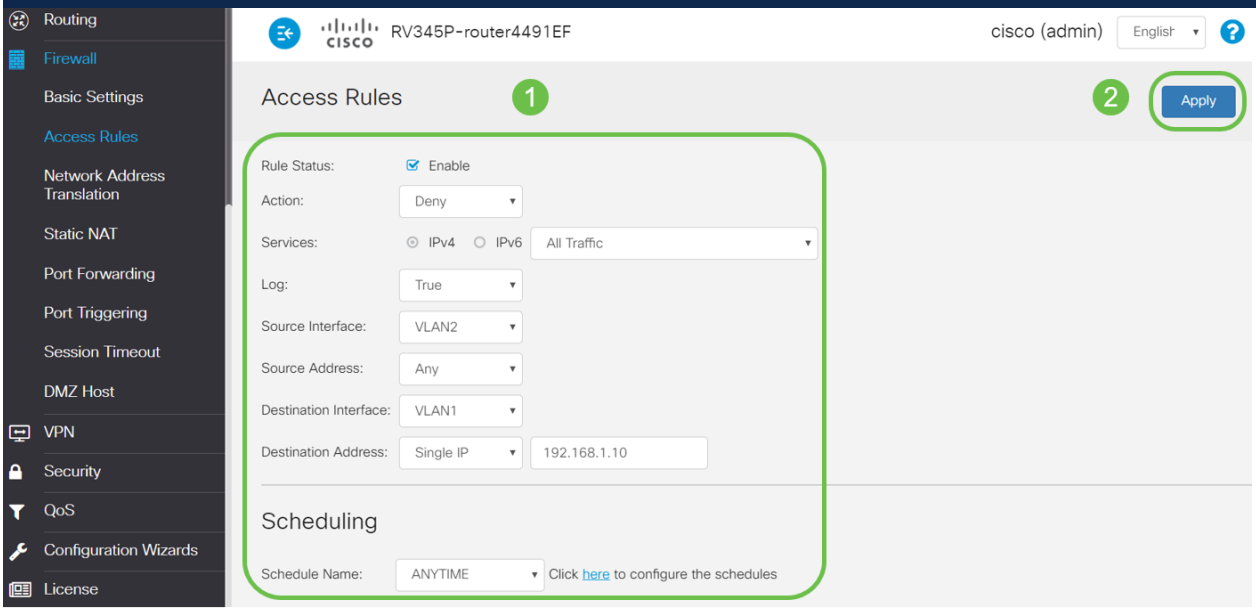
Stap 3

Configureer de parameters *van de toegangsregels*. Toepassen ACL om de server (IPv4) te beperken: 192.168.1.10/24) toegang van VLAN2-gebruikers. 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*

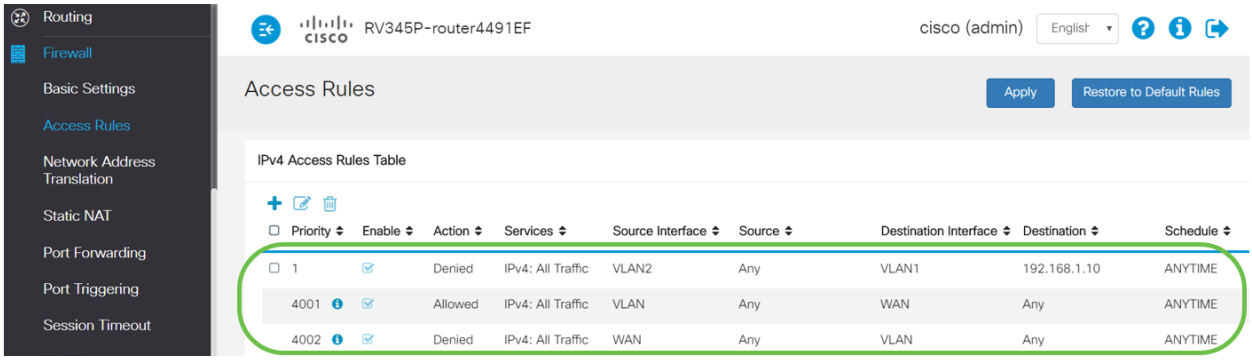
Klik op **Apply** (Toepassen).

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 4

De lijst *toegangsregels* bevat de volgende gegevens:



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 zoekvak van de computer en de optie **Opdrachtmelding** 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 toegangsregel op een Cisco RV34x Series router te configureren. Nu kunt u dat toepassen om een toegangsregel in uw netwerk te maken die uw behoeften zal passen!