Configuratie van poortdoorsturen/poortfiltering/NAT op RV34x Series routers

Doel

Leg het doel van port door te sturen en poort te openen en geef instructies om deze functies op uw RV34x Series router in te stellen.

- Vergelijken van poortdoorsturen en poortfiltering
- Poortdoorsturen en poortcontrole instellen
- Netwerkadresomzetting (NAT) instellen

Toepasselijke apparaten

- RV344x routerserie

Softwareversie

- 1.0.01.17

Vergelijken van poortdoorsturen en poortfiltering

Deze functies maken het voor sommige internetgebruikers mogelijk om toegang te hebben tot specifieke bronnen op uw netwerk, terwijl u de bronnen die u wilt privé houden, beschermd. Een paar voorbeelden van het gebruik van deze methode: het organiseren van web/e-mail servers, alarmsysteem en beveiligingscamera's (het terugsturen van de video naar een externe computer). Poortverzending opent poorten als reactie op inkomend verkeer voor een gespecificeerde service.

Een lijst van deze poorten en de beschrijving ervan worden ingesteld wanneer u de informatie in het gedeelte Service Management van de wizard invoert. Wanneer u deze instelt, kunt u niet hetzelfde poortnummer gebruiken voor zowel poort-verzenden als poort-triggen.

Poortdoorsturen

Poorttransport is een technologie die het publiek toegang tot services op netwerkapparaten op het Local Area Network (LAN) biedt door een specifieke poort te openen voor een service in reactie op inkomende verkeer. Dit zorgt ervoor dat de pakketten een duidelijk pad naar de beoogde bestemming hebben, wat voor snellere downloadsnelheden en minder latentie zorgt. Dit is ingesteld voor één computer op uw netwerk. U moet het IP-adres van de specifieke computer toevoegen en dit kan niet worden gewijzigd.

Dit is een statische handeling die een specifiek bereik van poorten opent dat u selecteert en niet wijzigt. Dit kan het veiligheidsrisico vergroten omdat de geconfigureerde poorten altijd open zijn.

Stel je voor dat een deur altijd open is op die poort naar dat apparaat dat het toegewezen werd.

Poortcontrole

Poorttrigeren is gelijkaardig aan poortverzending maar een beetje veiliger. Het verschil is dat de trekker niet altijd open is voor dat specifieke verkeer. Nadat een middel op uw LAN uitgaand verkeer door een slaghaven verstuurt, luistert de router naar binnenkomend verkeer door een gespecificeerde haven of havenbereik. Gevorderde havens worden gesloten wanneer er geen activiteit is, hetgeen de veiligheid vergroot. Een ander voordeel is dat meer dan één computer op uw netwerk deze poort op verschillende tijdstippen kan benaderen. U hoeft daarom niet het IP-adres van de computer te kennen dat het zal activeren. Dit gebeurt automatisch.

Denk je dat je iemand een pas geeft, maar er is een portier die je pas controleert telkens als je binnenkomt en de deur sluit tot de volgende persoon met een pas aankomt.

Poortdoorsturen en poortcontrole instellen

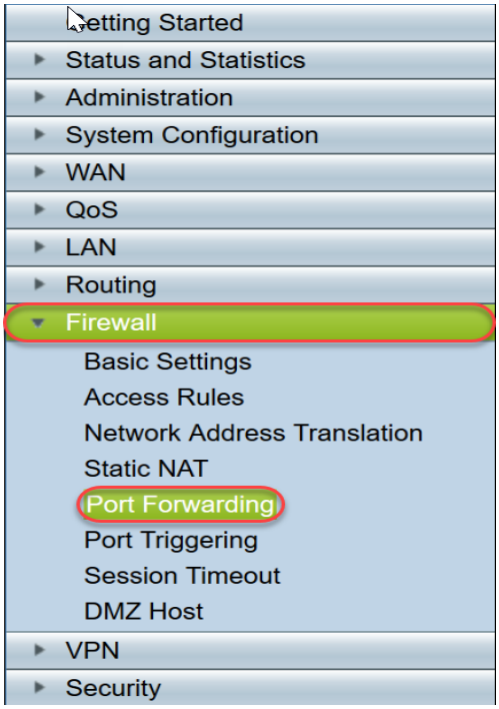
Poortdoorsturen

Om haven aan te passen die, volg deze stappen:

Stap 1. Meld u aan bij het programma voor webconfiguratie. Voer het IP-adres voor de router in de spatie-/adresbalk in. De browser waarschuwt dat de website onbetrouwbaar is. Ga verder naar de website. Klik hier voor meer informatie over deze stap.

Voer de gebruikersnaam en het wachtwoord voor de router in en klik op **Log in**. De standaard gebruikersnaam en wachtwoord zijn Cisco.

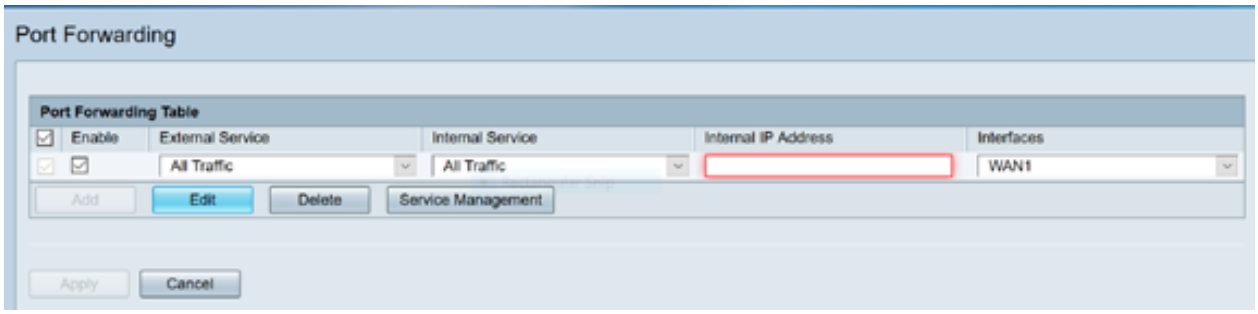
Stap 2.Klik in het hoofdmenu aan de linkerkant **op Firewall > Doorsturen van poorten**



Klik in de tabel Poortdoorsturen op **Add** of selecteer de rij en klik op **Bewerken** om het volgende te configureren:

Externe dienstverlening	Selecteer een externe service in de vervolgkeuzelijst. (Als een service niet in de lijst staat, kunt u de lijst toevoegen of wijzigen via de instructies in het gedeelte Service Management.)
Interne dienst	Selecteer een interne service in de vervolgkeuzelijst. (Als een service niet in de lijst staat, kunt u de lijst toevoegen of wijzigen via de instructies in het gedeelte Service Management.)
Intern IP-adres	Voer de interne IP-adressen van de server in.

Interfaces	Selecteer de interface uit de vervolgkeuzelijst om poort te gebruiken bij het verzenden.
Status	Schakel de poortverzendregel in of uit.

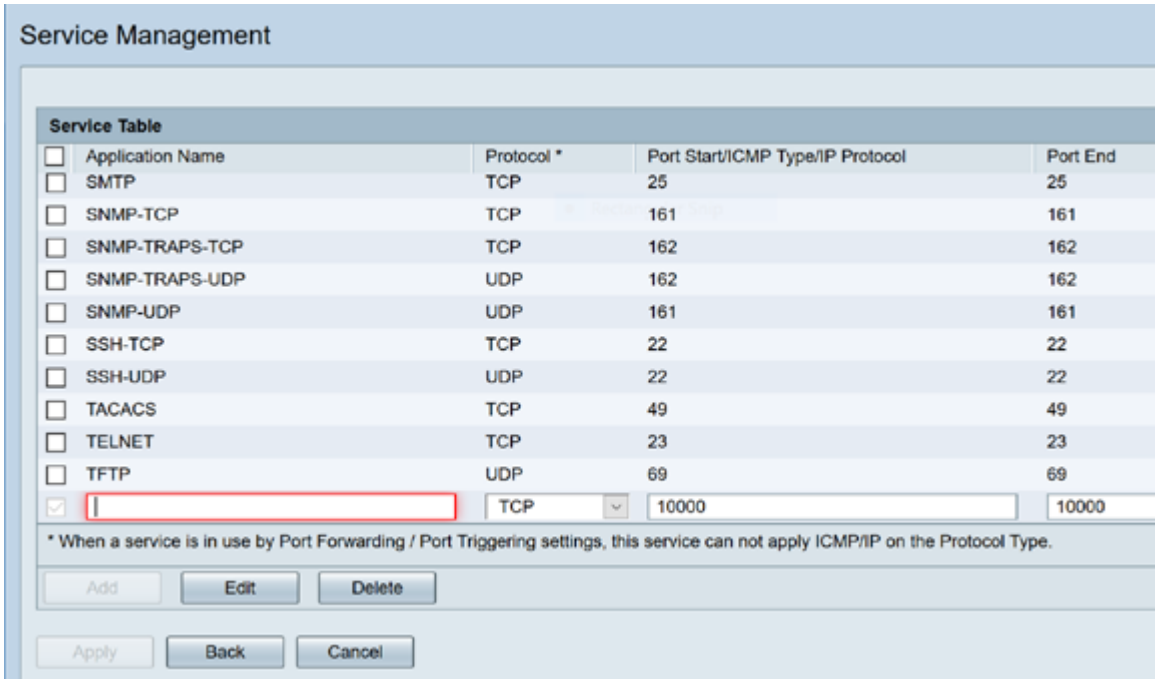


Een bedrijf hosts een webserver (met een intern IP-adres van 192.0.2.1) op hun LAN. Een poort-expediteits regel voor HTTP verkeer kan worden ingeschakeld. Dit zou verzoeken van het internet in dat netwerk mogelijk maken. Het bedrijf stelt het poortnummer 80 (HTTP) in dat naar IP-adres 192.0.2.1 wordt doorgestuurd, dan worden alle HTTP-verzoeken van externe gebruikers doorgestuurd naar 192.0.2.1. Het is ingesteld voor dat specifieke apparaat in het netwerk.

Stap 3.Klik op **Servicebeheer**

Klik in de Servicetabel op **Toevoegen** of selecteer een rij en klik op **Bewerken** om het volgende te configureren:

- Toepassingsnaam - naam van de service of toepassing
- Protocol - verplicht protocol. Raadpleeg de documentatie voor de service die u ontvangt
- Port Start/ICMP Type/IP-protocol - Bereik van poortnummers gereserveerd voor deze service
- Port End-of-life laatste nummer van de poort, gereserveerd voor deze service

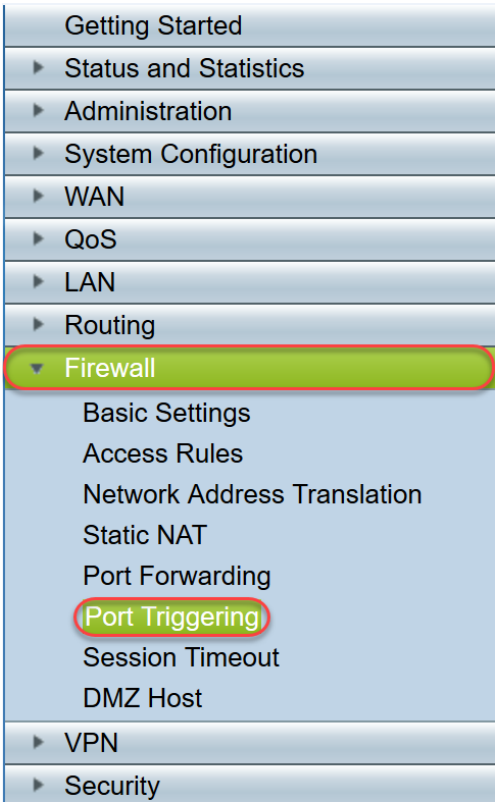


Stap 4. Klik op **Toepassen**

Poortcontrole

Om poort te configureren die trigeren, volgt u deze stappen:

Stap 1.Meld u aan bij het web configuratieprogramma. Klik in het hoofdmenu aan de linkerkant op **Firewall > Port Trigving**

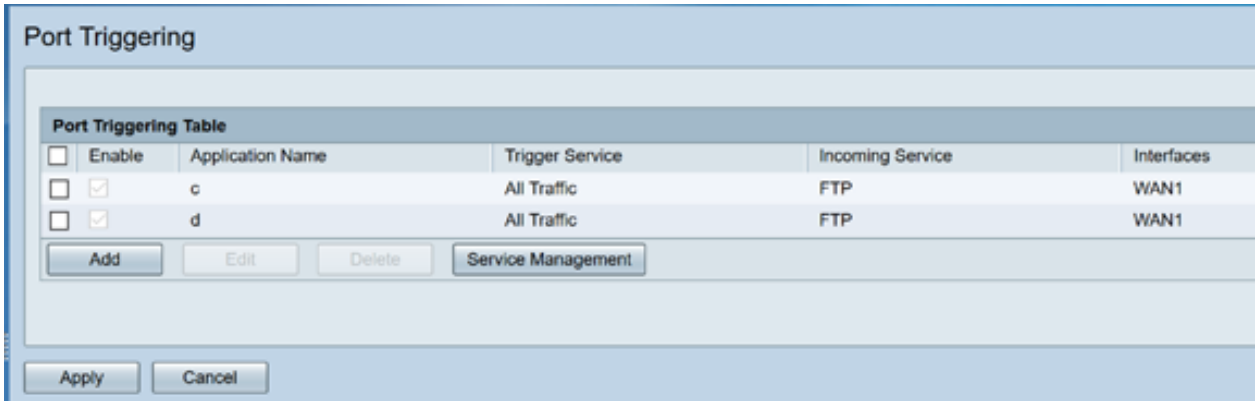


Stap 2. U kunt een service aan de poort die een triggertabel biedt toevoegen of bewerken door het volgende te configureren:

Toepassingsnaam	Voer de naam

	van de toepassing in.
triggerservice	Selecteer een service in de vervolgkeuzelijst. (Als een service niet in de lijst staat, kunt u de lijst toevoegen of wijzigen via de instructies in het gedeelte Service Management.)
Inkomende service	Selecteer een service in de vervolgkeuzelijst. (Als een service niet in de lijst staat, kunt u de lijst toevoegen of wijzigen via de instructies in het gedeelte Service Management.)
Interfaces	Selecteer de interface in de vervolgkeuzelijst.
Status	Schakel de poort-triggerregel in of uit.

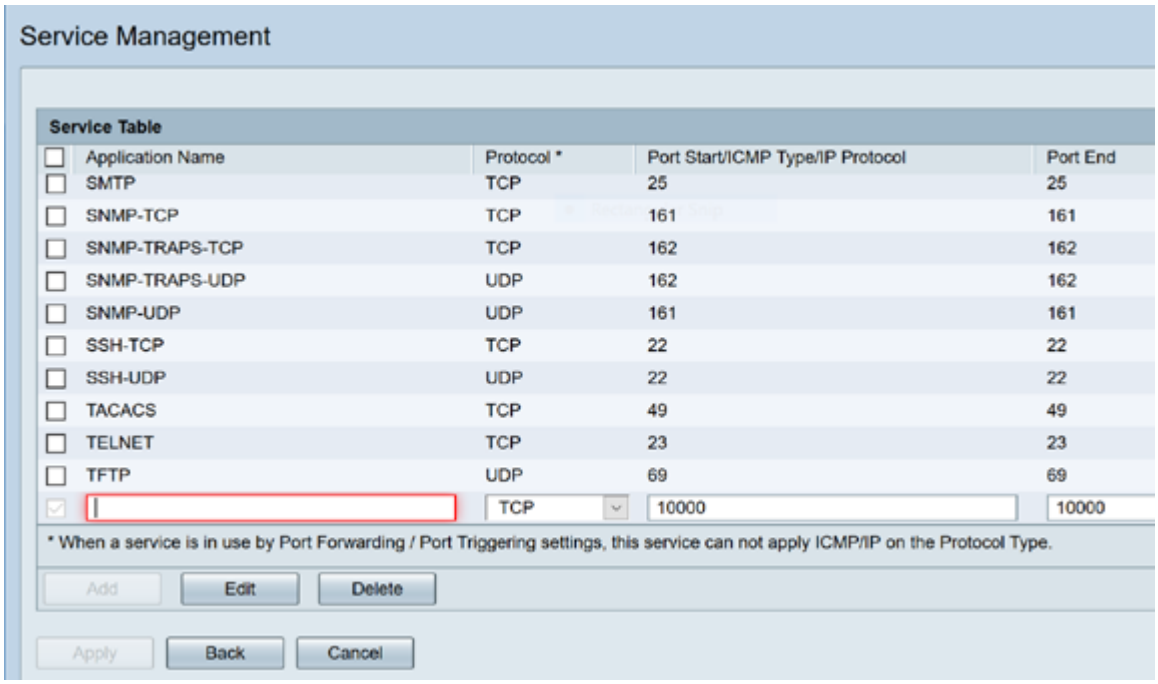
Klik op **Add** (of selecteer de rij en klik op **Bewerken**) en voer de volgende informatie in:



Stap 3. Klik op **Service Management** om een item in de lijst Service toe te voegen of te bewerken.

Klik in de Servicetabel op **Toevoegen** of **Bewerken** en kies het volgende:

- Toepassingsnaam - naam van de service of toepassing
- Protocol - verplicht protocol. Raadpleeg de documentatie voor de service die u ontvangt
- Port Start/ICMP Type/IP-protocol - Bereik van poortnummers gereserveerd voor deze service
- Port End-of-life laatste nummer van de poort, gereserveerd voor deze service



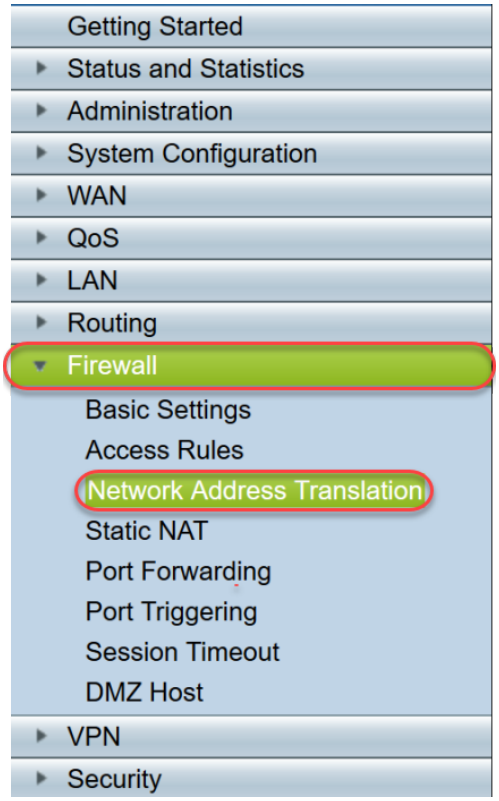
Stap 4. Klik op **Toepassen**

Netwerkadresomzetting

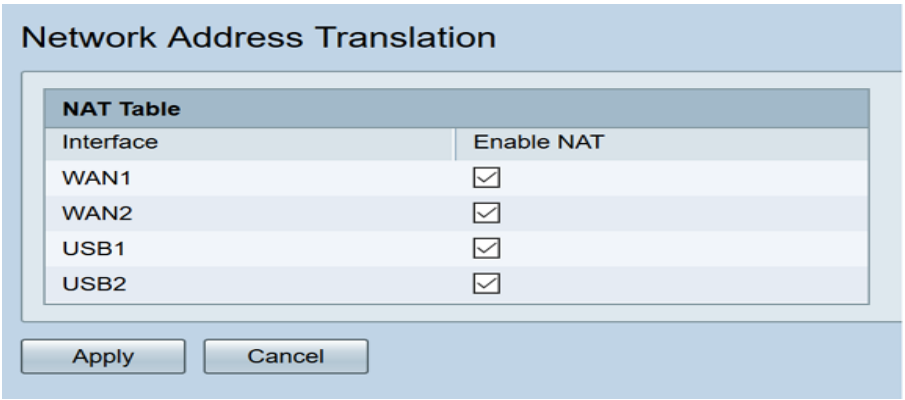
Network Address Translation (NAT) maakt privé IP-netwerken met niet-geregistreerde IP-adressen in staat om verbinding te maken met het openbare netwerk. Dit is een algemeen ingesteld protocol in de meeste netwerken. NAT vertaalt de privé IP-adressen van het interne netwerk naar openbare IP-adressen voordat pakketten naar het openbare netwerk worden doorgestuurd. Dit staat een groot aantal hosts op een intern netwerk toe om toegang tot het internet te krijgen via een beperkt aantal openbare IP-adressen. Dit helpt ook om de privé IP adressen tegen elke kwaadwillige aanval of ontdekking te beschermen aangezien de privé IP adressen verborgen worden gehouden.

Om NAT te configureren volgt u deze stappen

Stap 1.Klik op **Firewall> Netwerkadresomzetting**



Stap 2. In de NAT-tabel staat u NAT voor elke toepasselijke interface in de lijst in om dit mogelijk te maken



Stap 3. Klik op **Toepassen**

U hebt nu met succes ingesteld op het verzenden van poorten, het maken van poorten en NAT.

Overige bronnen

- Klik hier voor de configuratie van statische NAT
- Voor antwoorden op veel vragen over routers, inclusief de RV3xx-serie, klikt u hier
- Voor FAQ's in de RV34x-serie, klik hier
- Klik hier voor meer informatie over RV345 en RV345P
- Klik hier voor meer informatie over het configureren van servicebeheer in de RV34x-serie

Bekijk een video gerelateerd aan dit artikel...

Klik hier om andere Tech Talks uit Cisco te bekijken