Konfigurieren von Port Forwarding/Port Triggering/NAT auf Routern der Serie RV34x

Ziel

Erläutern des Zwecks der Port-Weiterleitung und der Port-Triggering und Anleitungen zum Einrichten dieser Funktionen auf dem Router der Serie RV34x

- Vergleich von Port Forwarding und Port Triggering
- Einrichten von Port Forwarding und Port Triggering
- Network Address Translation (NAT) einrichten

Anwendbare Geräte

- RV34x Router-Serie

Softwareversion

- 1.0.01.17

Vergleich von Port Forwarding und Port Triggering

Diese Funktionen ermöglichen es einigen Internetbenutzern, auf bestimmte Ressourcen in Ihrem Netzwerk zuzugreifen, und schützen gleichzeitig die Ressourcen, die Sie privat halten möchten. Beispiele für die Verwendung dieser Methode: Hosten von Web-/E-Mail-Servern, Alarmsystem und Sicherheitskameras (zum Senden des Videos an einen externen Computer). Port Forwarding öffnet Ports als Antwort auf eingehenden Datenverkehr für einen angegebenen Service.

Eine Liste dieser Ports und deren Beschreibung werden eingerichtet, wenn Sie die Informationen im Abschnitt "Service Management" des Einrichtungs-Assistenten eingeben. Wenn Sie diese einrichten, können Sie nicht dieselbe Portnummer sowohl für die Port-Weiterleitung als auch für das Port-Triggering verwenden.

Port Forwarding

Port Forwarding ist eine Technologie, die den öffentlichen Zugriff auf Services auf Netzwerkgeräten im Local Area Network (LAN) ermöglicht, indem als Reaktion auf eingehenden Datenverkehr ein bestimmter Port für einen Service geöffnet wird. Dadurch wird sichergestellt, dass die Pakete über einen klaren Pfad zum beabsichtigten Ziel verfügen, der schnellere Download-Geschwindigkeiten und eine geringere Latenz ermöglicht. Diese Einstellung ist für einen einzelnen Computer im Netzwerk festgelegt. Sie müssen die IP-Adresse des jeweiligen Computers hinzufügen, und diese kann nicht geändert werden.

Dies ist eine statische Operation, die einen bestimmten Portbereich öffnet, den Sie auswählen und nicht ändern. Dies kann das Sicherheitsrisiko erhöhen, da die konfigurierten Ports immer offen sind.

Stellen Sie sich vor, an diesem Port ist immer eine Tür für das Gerät geöffnet, dem es zugewiesen wurde.

Port-Triggering

Port-Triggering ähnelt der Port-Weiterleitung, ist jedoch etwas sicherer. Der Unterschied besteht darin, dass der Trigger-Port nicht immer für diesen spezifischen Datenverkehr geöffnet ist. Nachdem eine Ressource im LAN ausgehenden Datenverkehr über einen Trigger-Port sendet, überwacht der Router eingehenden Datenverkehr über einen bestimmten Port oder Port-Bereich. Ausgelöste Ports werden geschlossen, wenn keine Aktivität verzeichnet wird, was die Sicherheit erhöht. Ein weiterer Vorteil ist, dass mehr als ein Computer im Netzwerk zu unterschiedlichen Zeiten auf diesen Port zugreifen kann. Daher müssen Sie die IP-Adresse des Computers, der sie im Voraus auslöst, nicht kennen. Dies geschieht automatisch.

Denken Sie daran, dass Sie jemandem einen Pass geben, aber es gibt einen Türsteher, der Ihren Pass prüft jedes Mal, wenn Sie eintreten und dann schließt die Tür, bis die nächste Person mit einem Pass kommt.

Einrichten von Port Forwarding und Port Triggering

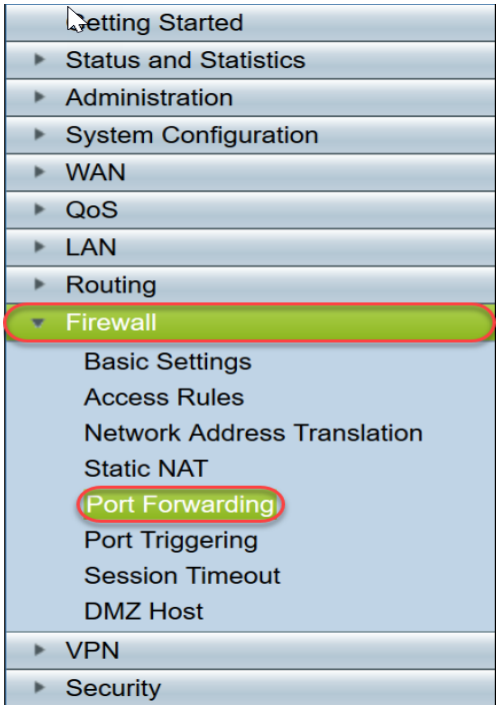
Port Forwarding

Um die Port-Weiterleitung zu konfigurieren, gehen Sie wie folgt vor:

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an. Geben Sie die IP-Adresse für den Router in die Suchleiste ein. Der Browser gibt möglicherweise eine Warnung aus, dass die Website nicht vertrauenswürdig ist. Weiter zur Website. Weitere Informationen zu diesem Schritt erhalten Sie hier.

Geben Sie den Benutzernamen und das Kennwort für den Router ein, und klicken Sie auf **Anmelden**. Der Standard-Benutzername und das Kennwort lautet cisco.

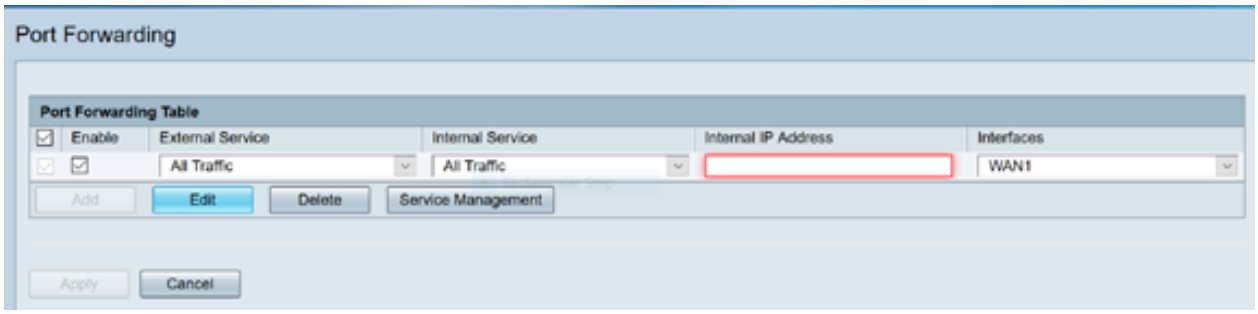
Schritt 2.Klicken Sie im Hauptmenü auf der linken Seite **auf Firewall > Port Forwarding**



Klicken Sie in der Port Forwarding Table (Port-Weiterleitungstabelle) auf **Hinzufügen**, oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**, um Folgendes zu konfigurieren:

Externer Service	Wählen Sie einen externen Service aus der Dropdown-Liste aus. (Wenn ein Service nicht aufgeführt ist, können Sie die Liste hinzufügen oder ändern, indem Sie die Anweisungen im Abschnitt "Service Management" befolgen.)
Interner Service	Wählen Sie einen internen Service aus der Dropdown-Liste aus. (Wenn ein Service nicht aufgeführt ist, können Sie die Liste hinzufügen oder ändern, indem Sie die Anweisungen im Abschnitt "Service Management"

	befolgen.)
Interne IP-Adresse	Geben Sie die internen IP-Adressen des Servers ein.
Schnittstellen	Wählen Sie die Schnittstelle aus der Dropdown-Liste aus, um die Port-Weiterleitung anzuwenden.
Status	Aktivieren oder Deaktivieren der Port Forwarding-Regel.

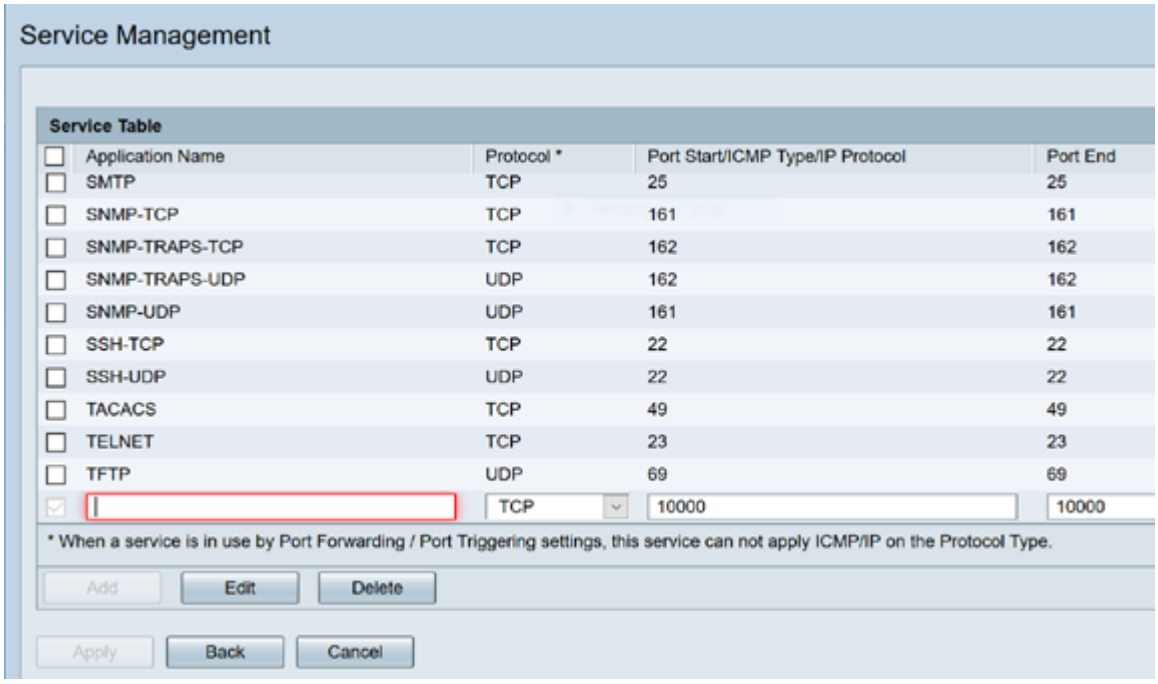


Ein Unternehmen hostet beispielsweise einen Webserver (mit der internen IP-Adresse 192.0.2.1) in seinem LAN. Eine Port Forwarding-Regel für HTTP-Datenverkehr könnte aktiviert werden. Dies würde Anfragen aus dem Internet in dieses Netzwerk erlauben. Das Unternehmen legt die Portnummer 80 (HTTP) fest, die an die IP-Adresse 192.0.2.1 weitergeleitet werden soll. Anschließend werden alle HTTP-Anfragen von externen Benutzern an 192.0.2.1 weitergeleitet. Sie ist für das jeweilige Gerät im Netzwerk eingerichtet.

Schritt 3.Klicken Sie auf **Service Management**

Klicken Sie in der Service-Tabelle auf **Hinzufügen**, oder wählen Sie eine Zeile aus, und klicken Sie auf **Bearbeiten**, und konfigurieren Sie Folgendes:

- Anwendungsname - Name des Services oder der Anwendung
- Protokoll - Erforderliches Protokoll. Weitere Informationen zu dem Dienst, den Sie hosten, finden Sie in der Dokumentation.
- Port Start/ICMP Type/IP Protocol - Bereich der für diesen Service reservierten Portnummern
- Port-Ende - Letzte Nummer des Ports, reserviert für diesen Service

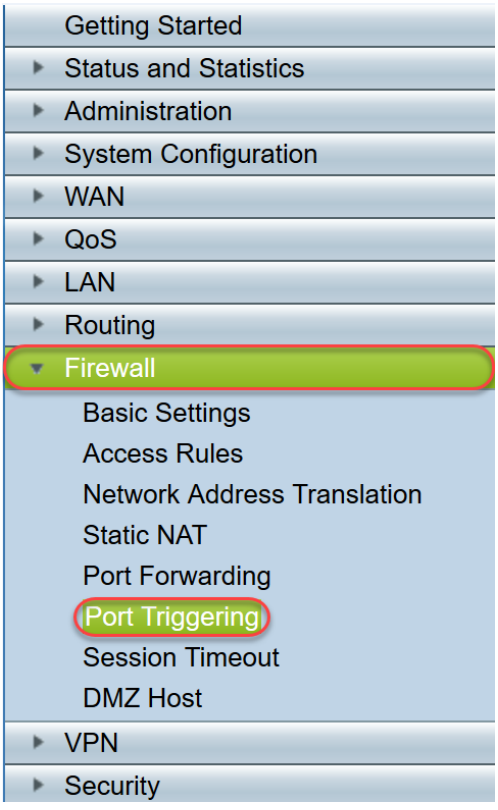


Schritt 4: Klicken Sie auf **Übernehmen**

Port-Triggering

Um das Port-Triggering zu konfigurieren, gehen Sie wie folgt vor:

Schritt 1:Melden Sie sich beim Webkonfigurationsprogramm an. Klicken Sie im Hauptmenü links auf **Firewall > Port Triggering.**

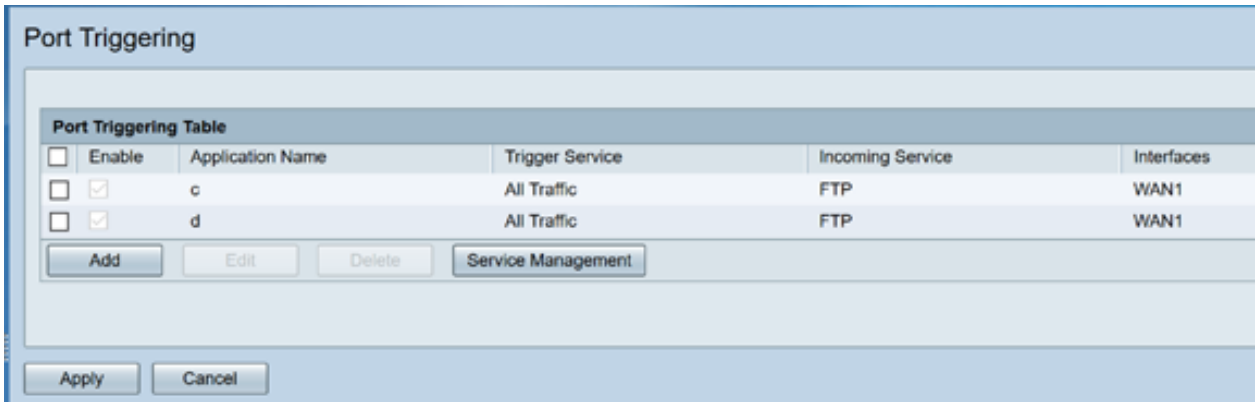


Schritt 2: Konfigurieren Sie Folgendes, um der Port-Auslösetabelle einen Dienst hinzuzufügen oder zu bearbeiten:

Anwendungsname	Geben Sie den

	Namen der Anwendung ein.
Trigger-Service	Wählen Sie einen Service aus der Dropdown-Liste aus. (Wenn ein Service nicht aufgeführt ist, können Sie die Liste hinzufügen oder ändern, indem Sie die Anweisungen im Abschnitt "Service Management" befolgen.)
Eingehender Service	Wählen Sie einen Service aus der Dropdown-Liste aus. (Wenn ein Service nicht aufgeführt ist, können Sie die Liste hinzufügen oder ändern, indem Sie die Anweisungen im Abschnitt "Service Management" befolgen.)
Schnittstellen	Wählen Sie die Schnittstelle aus der Dropdown-Liste aus.
Status	Aktivieren oder Deaktivieren der Regel für das Port-Triggering.

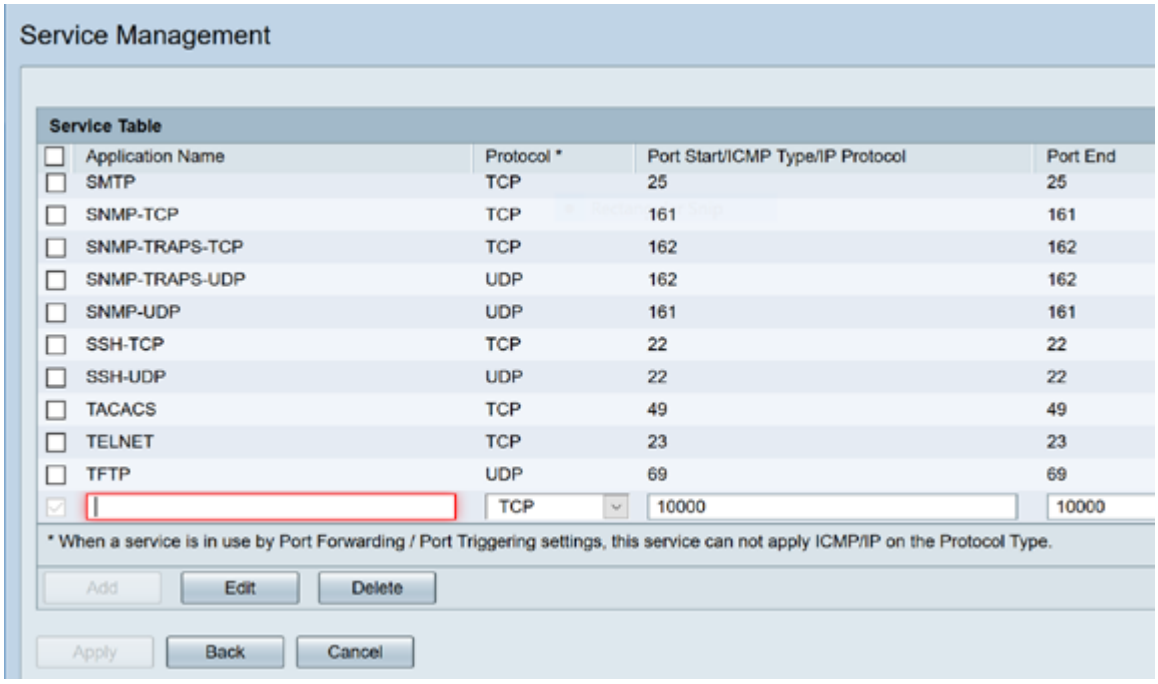
Klicken Sie auf **Hinzufügen** (oder wählen Sie die Zeile aus und klicken Sie auf **Bearbeiten**), und geben Sie die folgenden Informationen ein:



Schritt 3: Klicken Sie auf **Service Management**, um einen Eintrag in der Liste Dienste hinzuzufügen oder zu bearbeiten.

Klicken Sie in der Service-Tabelle auf **Hinzufügen** oder **Bearbeiten**, und konfigurieren Sie Folgendes:

- Anwendungsname - Name des Services oder der Anwendung
- Protokoll - Erforderliches Protokoll. Weitere Informationen zu dem Dienst, den Sie hosten, finden Sie in der Dokumentation.
- Port Start/ICMP Type/IP Protocol - Bereich der für diesen Service reservierten Portnummern
- Port-Ende - Letzte Nummer des Ports, reserviert für diesen Service



Schritt 4.Klicken Sie auf **Übernehmen**

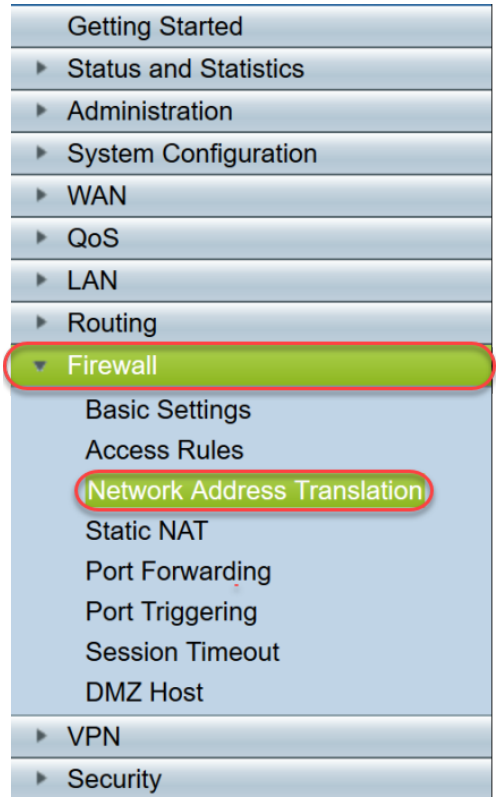
Network Address Translation

Network Address Translation (NAT) ermöglicht privaten IP-Netzwerken mit nicht registrierten IP-Adressen die Verbindung mit dem öffentlichen Netzwerk. Dies ist ein in den meisten Netzwerken allgemein konfiguriertes Protokoll. NAT übersetzt die privaten IP-Adressen des internen Netzwerks in öffentliche IP-Adressen, bevor Pakete an das öffentliche Netzwerk weitergeleitet werden. Dadurch kann eine große Anzahl von Hosts in einem internen

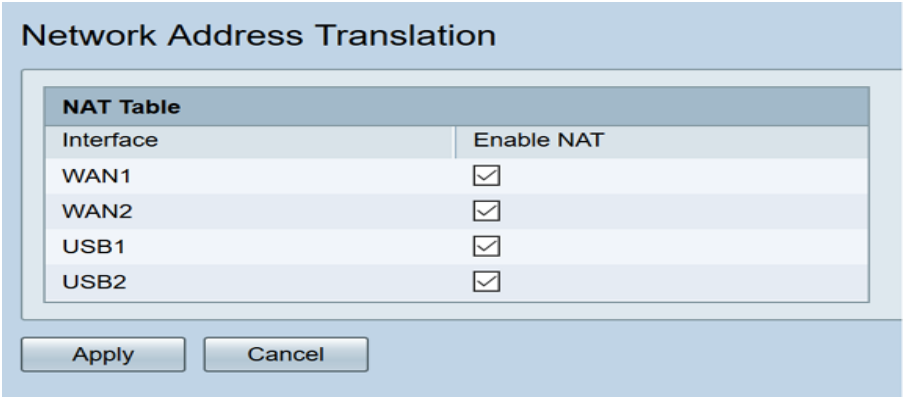
Netzwerk über eine begrenzte Anzahl öffentlicher IP-Adressen auf das Internet zugreifen. Dies trägt auch dazu bei, die privaten IP-Adressen vor bösartigen Angriffen oder schädlichen Erkennungen zu schützen, da die privaten IP-Adressen verborgen bleiben.

Führen Sie die folgenden Schritte aus, um NAT zu konfigurieren.

Schritt 1: Klicken Sie auf **Firewall > Network Address Translation**



Schritt 2: Aktivieren Sie in der NAT-Tabelle für jede entsprechende Schnittstelle in der Liste die Option NAT aktivieren, um



Schritt 3: Klicken Sie auf **Übernehmen**

Sie haben jetzt erfolgreich Port Forwarding, Port Triggering und NAT konfiguriert.

Weitere Ressourcen

- Zur Konfiguration der statischen NAT klicken Sie hier.
- Antworten auf viele Fragen zu Routern, einschließlich der Serie RV3xx, finden Sie hier
- Häufig gestellte Fragen zur Serie RV34x finden Sie hier.
- Weitere Informationen zu RV345 und RV345P erhalten Sie hier.

- Weitere Informationen zur Konfiguration der Service-Verwaltung für die Serie RV34x erhalten Sie hier.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.