

Konfigurieren von Port Forwarding und Port Triggering in Routern der Serien RV160 und RV260

Inhaltsverzeichnis

- [Ziel](#)
- [Anwendbare Geräte | Firmware-Version](#)
- [Einführung](#)
- [Konfigurieren der Port-Weiterleitung](#)
- [Konfigurieren von Port-Triggering](#)

Ziel

In diesem Artikel wird erläutert, wie die Port-Weiterleitung und die Port-Triggering auf den Routern RV160 und RV260 konfiguriert werden.

Anwendbare Geräte | Firmware-Version

RV160 | 1.0.00.13

RV260 | 1.0.00.13

Einführung

Port Forwarding und Port Triggering sind Funktionen, die es einigen Internetbenutzern ermöglichen, auf bestimmte Ressourcen in Ihrem Netzwerk zuzugreifen und gleichzeitig die Ressourcen zu schützen, die Sie privat halten möchten.

Die Port-Weiterleitung ermöglicht den öffentlichen Zugriff auf Services auf Netzwerkgeräten im Local Area Network (LAN), indem ein bestimmter Port oder Port-Bereich für einen Dienst, z. B. ein Dateiübertragungsprotokoll (FTP), geöffnet wird. Port Forwarding öffnet einen Port-Bereich für Dienste wie Internet-Gaming, das alternative Ports für die Kommunikation zwischen dem Server und dem LAN-Host verwendet.

Mit Port-Triggering kann ein angegebener Port oder Port-Bereich für eingehenden Datenverkehr geöffnet werden, nachdem der Benutzer ausgehenden Datenverkehr über den Trigger-Port sendet. Über das Port-Triggering kann das Gerät ausgehende Daten auf bestimmte Portnummern überwachen. Das Gerät ruft die IP-Adresse des Clients zurück, der die übereinstimmenden Daten gesendet hat. Wenn die angeforderten Daten über das Gerät zurückgegeben werden, werden die Daten mithilfe der IP-Adressierungs- und Port-Zuordnungsregeln an den entsprechenden Client gesendet.

Weitere Informationen zur Port-Weiterleitung und zum Port-Triggering erhalten Sie [hier](#).

Konfigurieren der Port-Weiterleitung

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

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an. Geben Sie den Benutzernamen und das Kennwort für den Router ein, und klicken Sie auf **Anmelden**. Der Standardbenutzername und das Standardkennwort lautet *cisco*.

In diesem Artikel wird der RV260 zum Konfigurieren der Port-Weiterleitung verwendet. Die Konfiguration kann je nach verwendetem Modell variieren.



Router

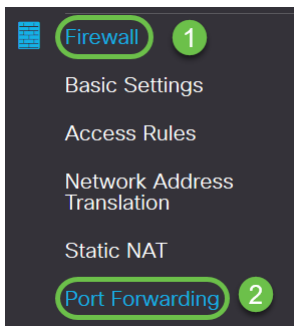
Username **1**

Password **2**

English **3**

Login **3**

Schritt 2: Klicken Sie auf **Firewall > Port Forwarding**.

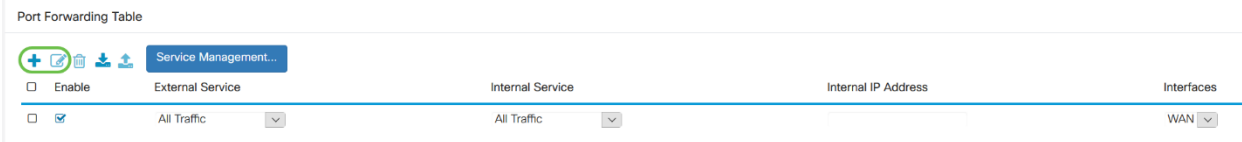


Schritt 3: Klicken Sie in der Port Forwarding Table (Tabelle für die Portweiterleitung) auf **das Symbol hinzufügen**, oder wählen Sie die Zeile aus, und klicken Sie auf das **Bearbeitungssymbol**, und konfigurieren Sie Folgendes:

Aktivieren	Aktivieren, um Port Forwarding zu aktivieren
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-Adressen	Geben Sie die internen IP-Adressen des Servers ein.
Schnittstellen	Wählen Sie die Schnittstelle aus der Dropdown-Liste aus, um die Port-

Weiterleitung anzuwenden auf

Port Forwarding Table

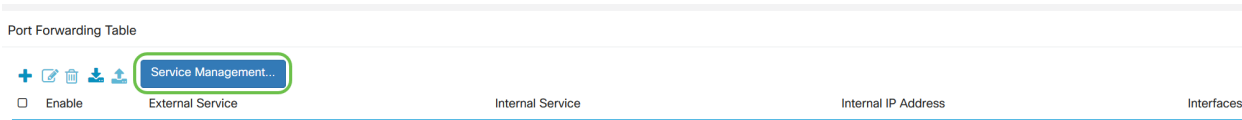


<input type="checkbox"/>	Enable	External Service	Internal Service	Internal IP Address	Interfaces
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All Traffic <input type="text" value="v"/>	All Traffic <input type="text" value="v"/>		WAN <input type="text" value="v"/>

Um einen Eintrag in der Liste "Service" hinzuzufügen oder zu bearbeiten, gehen Sie wie folgt vor:

Schritt 4: Klicken Sie auf **Service Management**.

Port Forwarding Table



<input type="checkbox"/>	Enable	External Service	Internal Service	Internal IP Address	Interfaces
--------------------------	--------	------------------	------------------	---------------------	------------

Schritt 5: Klicken Sie im *Service-Management* auf das **Symbol Hinzufügen**, oder wählen Sie eine Zeile aus, und klicken Sie auf das **Symbol Bearbeiten**.

Konfigurieren Sie Folgendes:

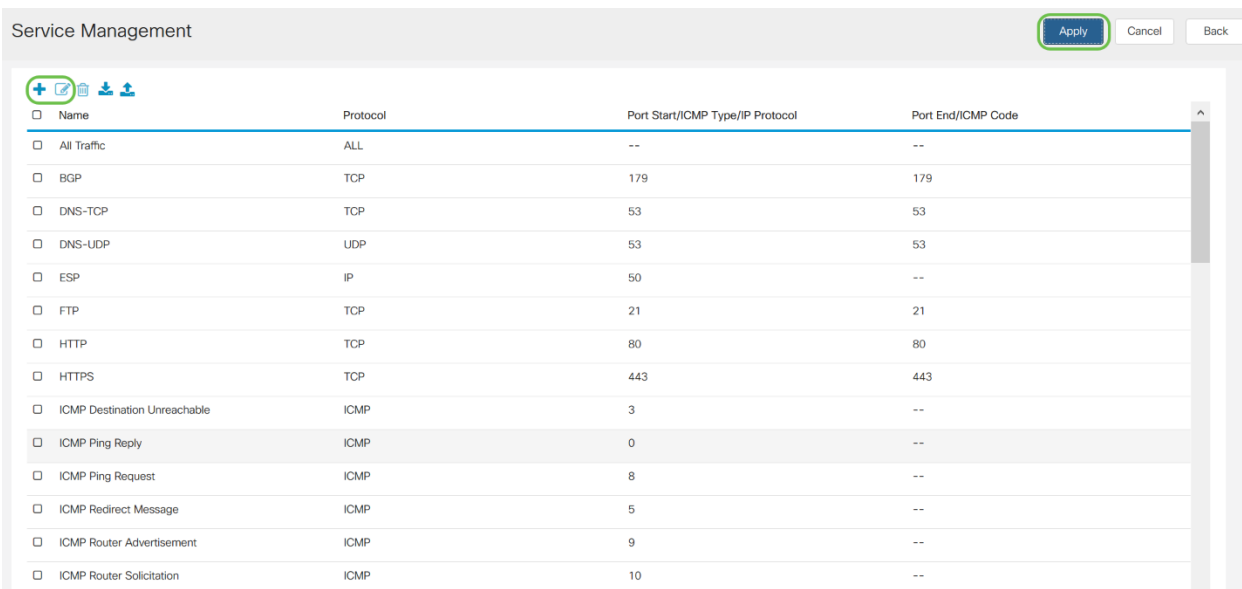
Anwendungsname: Name des Diensts oder der Anwendung.

Protokoll - Pflichtprotokoll. In der Dokumentation zu dem Dienst, den Sie hosten, nachsehen.

Port Start/ICMP Type/IP Protocol - Bereich der für diesen Service reservierten Portnummern.

Port-Ende - Letzte Nummer des Ports, der für diesen Service reserviert ist.

Service Management



<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80
<input type="checkbox"/>	HTTPS	TCP	443	443
<input type="checkbox"/>	ICMP Destination Unreachable	ICMP	3	--
<input type="checkbox"/>	ICMP Ping Reply	ICMP	0	--
<input type="checkbox"/>	ICMP Ping Request	ICMP	8	--
<input type="checkbox"/>	ICMP Redirect Message	ICMP	5	--
<input type="checkbox"/>	ICMP Router Advertisement	ICMP	9	--
<input type="checkbox"/>	ICMP Router Solicitation	ICMP	10	--

Um einen Service hinzuzufügen, klicken Sie auf das **Pluszeichen** und konfigurieren Sie Name, Protokoll, Port Start/ICMP Type/IP Protocol und Port End/ICMP Code.

Service Management Apply Cancel Back

<input type="checkbox"/>	RTSP-UDP	UDP	554	554
<input type="checkbox"/>	SFTP	TCP	115	115
<input type="checkbox"/>	SIP-TCP	TCP	5060	5060
<input type="checkbox"/>	SIP-UDP	UDP	5060	5060
<input type="checkbox"/>	SMTP	TCP	25	25
<input type="checkbox"/>	SNMP-TCP	TCP	161	161
<input type="checkbox"/>	SNMP-TRAPS-TCP	TCP	162	162
<input type="checkbox"/>	SNMP-TRAPS-UDP	UDP	162	162
<input type="checkbox"/>	SNMP-UDP	UDP	161	161
<input type="checkbox"/>	SSH-TCP	TCP	22	22
<input type="checkbox"/>	SSH-UDP	UDP	22	22
<input type="checkbox"/>	TACACS	TCP	49	49
<input type="checkbox"/>	TELNET	TCP	23	23
<input type="checkbox"/>	TFTP	UDP	69	69
<input type="checkbox"/>	<input type="text"/>	TCP	1000	1000

Um einen Dienst zu bearbeiten, markieren Sie eine Zeile, und klicken Sie auf das **Bearbeitungssymbol**, um die Felder wie unten dargestellt zu konfigurieren.

Service Management Apply

<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input checked="" type="checkbox"/>	<input type="text"/>	TCP	21	21
<input type="checkbox"/>	HTTP	All	80	80
<input type="checkbox"/>	HTTPS	TCP&UDP	443	443
<input type="checkbox"/>	ICMP Destination Unreachable	TCP	3	--
<input type="checkbox"/>	ICMP Ping Reply	UDP	0	--
<input type="checkbox"/>		IP		
<input type="checkbox"/>		ICMP		

In diesem Beispiel ist der FTP-Dienst ausgewählt.

Schritt 6: Klicken Sie auf **Übernehmen**.

Port Forwarding Apply Cancel

Port Forwarding Table

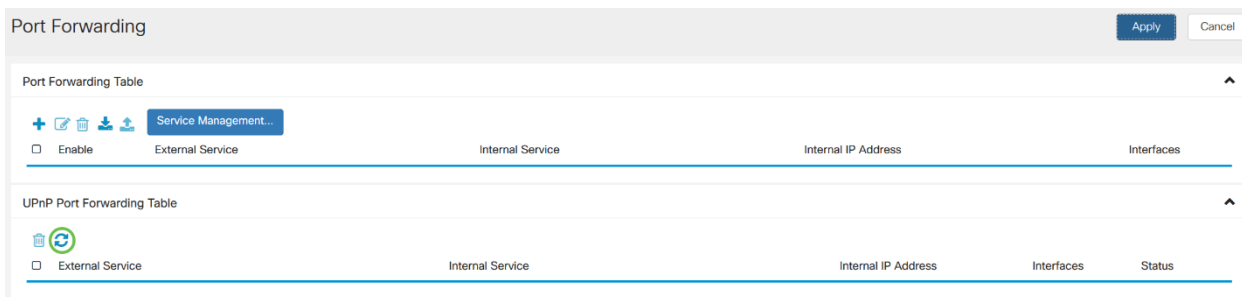
Service Management...

<input type="checkbox"/>	Enable	External Service	Internal Service	Internal IP Address	Interfaces
<input type="checkbox"/>					

UPnP Port Forwarding Table

<input type="checkbox"/>	External Service	Internal Service	Internal IP Address	Interfaces	Status
<input type="checkbox"/>					

Schritt 7: Klicken Sie in der Tabelle Universal Plug and Play (UPnP) Port Forwarding (UPnP) auf das **Aktualisierungssymbol**, um die Daten zu aktualisieren. Die Port Forwarding-Regeln für UPnP werden von der UPnP-Anwendung dynamisch hinzugefügt.



Konfigurieren von Port-Triggering

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

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an. Geben Sie den Benutzernamen und das Kennwort für den Router ein, und klicken Sie auf **Anmelden**. Der Standardbenutzername und das Standardkennwort lautet *cisco*.



Router

Username **1**

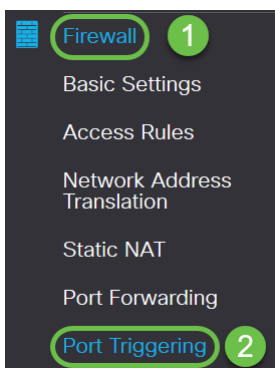
Password **2**

English **3**

Login **3**

In diesem Artikel wird der RV260 zum Konfigurieren von Port-Triggering verwendet. Die Konfiguration kann je nach verwendetem Modell variieren.

Schritt 2: Klicken Sie auf **Firewall > Port Triggering**.

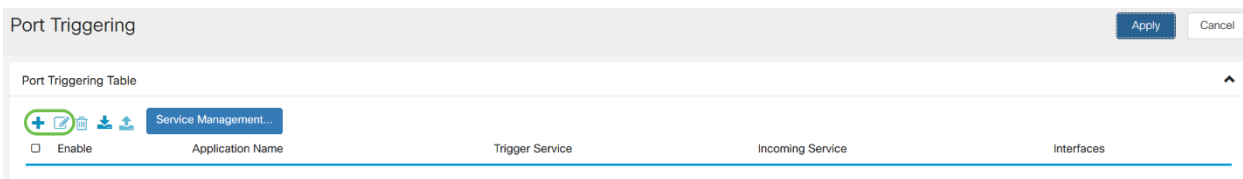


Schritt 3: Um der Port-Auslösetabelle einen Dienst hinzuzufügen oder zu bearbeiten, konfigurieren Sie Folgendes:

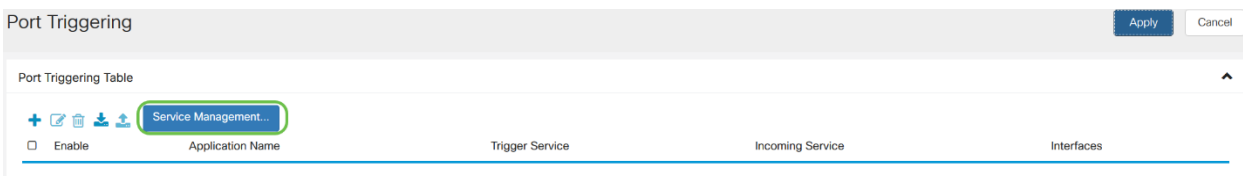
Klicken Sie auf **Symbol hinzufügen** (oder wählen Sie die Zeile aus, klicken Sie auf **das Symbol**

Bearbeiten, und geben Sie die Informationen ein:

Aktivieren	Aktivieren von Port-Triggering
Anwendungsname	Geben Sie den Namen der Anwendung ein. 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.)
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.



Schritt 4: Klicken Sie auf **Service Management**, um einen Eintrag in der Liste Dienste hinzuzufügen oder zu bearbeiten.



Schritt 5: Klicken Sie im *Service-Management* auf das **Symbol hinzufügen**, oder wählen Sie die Zeile aus, und klicken Sie auf das **Symbol Bearbeiten**.

Konfigurieren Sie Folgendes:

Anwendungsname: Name des Diensts oder der Anwendung.

Protokoll - Pflichtprotokoll. In der Dokumentation zu dem Dienst, den Sie hosten, nachsehen.

Port Start/ICMP Type/IP Protocol - Bereich der für diesen Service reservierten Portnummern.

Port-Ende - Letzte Nummer des Ports, der für diesen Service reserviert ist.

Service Management Apply Cancel Back

+ ✎ 🗑️ 📄 📥 📤

<input type="checkbox"/> Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/> All Traffic	ALL	--	--
<input type="checkbox"/> BGP	TCP	179	179
<input type="checkbox"/> DNS-TCP	TCP	53	53
<input type="checkbox"/> DNS-UDP	UDP	53	53
<input type="checkbox"/> ESP	IP	50	--
<input type="checkbox"/> FTP	TCP	21	21
<input type="checkbox"/> HTTP	TCP	80	80
<input type="checkbox"/> HTTPS	TCP	443	443
<input type="checkbox"/> ICMP Destination Unreachable	ICMP	3	--
<input type="checkbox"/> ICMP Ping Reply	ICMP	0	--
<input type="checkbox"/> ICMP Ping Request	ICMP	8	--
<input type="checkbox"/> ICMP Redirect Message	ICMP	5	--
<input type="checkbox"/> ICMP Router Advertisement	ICMP	9	--
<input type="checkbox"/> ICMP Router Solicitation	ICMP	10	--

Um einen Service hinzuzufügen, klicken Sie auf das *Pluszeichen* und konfigurieren Sie *Name*, *Protokoll*, *Port Start/ICMP Type/IP Protocol* und *Port End/ICMP Code*.

Service Management Apply Cancel Back

+ ✎ 🗑️ 📄 📥 📤

<input type="checkbox"/> RTSP-UDP	UDP	554	554
<input type="checkbox"/> SFTP	TCP	115	115
<input type="checkbox"/> SIP-TCP	TCP	5060	5060
<input type="checkbox"/> SIP-UDP	UDP	5060	5060
<input type="checkbox"/> SMTP	TCP	25	25
<input type="checkbox"/> SNMP-TCP	TCP	161	161
<input type="checkbox"/> SNMP-TRAPS-TCP	TCP	162	162
<input type="checkbox"/> SNMP-TRAPS-UDP	UDP	162	162
<input type="checkbox"/> SNMP-UDP	UDP	161	161
<input type="checkbox"/> SSH-TCP	TCP	22	22
<input type="checkbox"/> SSH-UDP	UDP	22	22
<input type="checkbox"/> TACACS	TCP	49	49
<input type="checkbox"/> TELNET	TCP	23	23
<input type="checkbox"/> TFTP	UDP	69	69
<input type="checkbox"/>	TCP	1000	1000

Um einen Dienst zu bearbeiten, markieren Sie eine Zeile, und klicken Sie auf das *Bearbeitungssymbol*, um die Felder wie unten dargestellt zu konfigurieren.

