

Configurazione dell'inoltro e dell'attivazione delle porte nei router RV160 e RV260

Sommario

- [Obiettivo](#)
- [Dispositivi interessati | Versione firmware](#)
- [Introduzione](#)
- [Configura inoltro porte](#)
- [Configura attivazione porta](#)

Obiettivo

L'obiettivo di questo articolo è mostrare come configurare l'inoltro delle porte e l'attivazione delle porte sui router RV160 e RV260.

Dispositivi interessati | Versione firmware

RV160 | 1.0.00.13

RV260 | 1.0.00.13

Introduzione

L'inoltro delle porte e l'attivazione delle porte sono funzionalità che consentono ad alcuni utenti Internet di accedere a risorse specifiche della rete, proteggendo al contempo le risorse che si desidera mantenere private.

L'inoltro delle porte consente l'accesso pubblico ai servizi dei dispositivi di rete sulla LAN (Local Area Network) tramite l'apertura di una porta o di un intervallo di porte specifici per un servizio, ad esempio il protocollo FTP (File Transfer Protocol). L'inoltro delle porte apre un intervallo di porte per servizi quali i giochi su Internet che utilizzano porte alternative per la comunicazione tra il server e l'host LAN.

L'attivazione delle porte consente l'apertura di una porta o di un intervallo di porte specificato per il traffico in entrata dopo l'invio del traffico in uscita da parte dell'utente tramite la porta di attivazione. L'attivazione delle porte consente al dispositivo di monitorare i dati in uscita per numeri di porta specifici. Il dispositivo richiama l'indirizzo IP del client che ha inviato i dati corrispondenti. Quando i dati richiesti ritornano attraverso il dispositivo, vengono inviati al client appropriato utilizzando le regole di mappatura delle porte e degli indirizzi IP.

Per ulteriori informazioni sull'inoltro e l'attivazione delle porte, fare clic [qui](#).

Configura inoltro porte

Per configurare l'inoltro delle porte, attenersi alla seguente procedura:

Passaggio 1. Accedere all'utility di configurazione Web. Immettere il nome utente e la password per il router e fare clic su **Login**. Il nome utente e la password predefiniti sono *cisco*.

In questo articolo, utilizzeremo la RV260 per configurare l'inoltro delle porte. La configurazione può variare a seconda del modello utilizzato.



Router

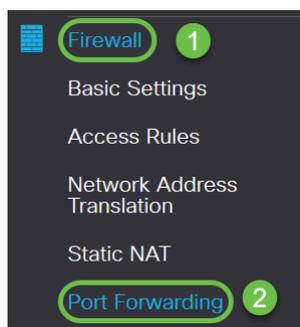
Username **1**

Password **2**

English **3**

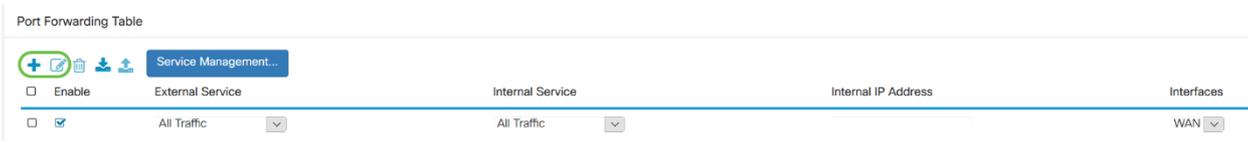
Login **3**

Passaggio 2. Fare clic su **Firewall > Inoltro porte**.



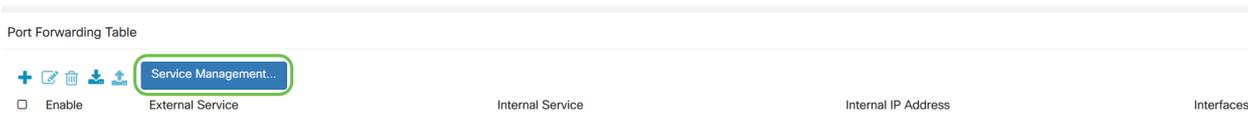
Passaggio 3. Nella tabella Inoltro porta, fare clic su **Aggiungi icona** o selezionare la riga e fare clic su **Modifica icona**) e configurare quanto segue:

Attiva	Selezionare Enable per abilitare l'inoltro delle porte
Servizio esterno	Selezionare un servizio esterno dall'elenco a discesa. Se un servizio non è presente nell'elenco, è possibile aggiungerlo o modificarlo seguendo le istruzioni della sezione Gestione servizi.
Servizio interno	Selezionare un servizio interno dall'elenco a discesa. Se un servizio non è presente nell'elenco, è possibile aggiungerlo o modificarlo seguendo le istruzioni della sezione Gestione servizi.
Indirizzi IP interni	Immettere gli indirizzi IP interni del server
Interfacce	Selezionare l'interfaccia dall'elenco a discesa per applicare l'inoltro delle porte



Per aggiungere o modificare una voce nell'elenco dei servizi, eseguire la procedura seguente:

Passaggio 4. Fare clic su **Gestione assistenza**.



Passaggio 5. In *Service Management* fare clic su **Icona Aggiungi** o selezionare una riga e fare clic su **Icona Modifica**.

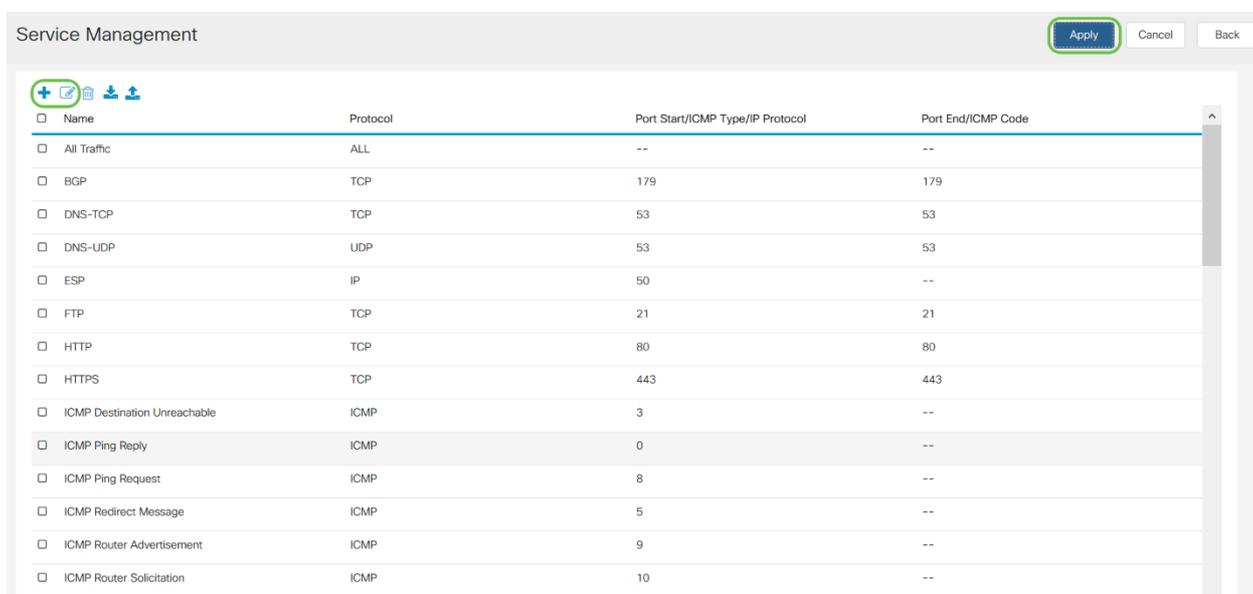
Configurare quanto segue:

Nome applicazione: nome del servizio o dell'applicazione.

Protocollo - Protocollo richiesto. Fare riferimento alla documentazione del servizio che si sta ospitando.

Port Start/ICMP Type/IP Protocol: intervallo di numeri di porta riservati per questo servizio.

Port End: ultimo numero della porta riservata per il servizio.



Per aggiungere un servizio, fare clic sull'**icona con il segno più** e configurare Nome, Protocollo, Porta Start/ICMP Tipo/Protocollo IP e Porta End/Codice ICMP.

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

Per modificare un servizio, selezionare una riga e fare clic sull'icona **Modifica** per configurare i campi come mostrato di seguito.

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"/>	FTP	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 questo esempio, è selezionato FTP service.

Passaggio 6. Fare clic su **Applica**.

Port Forwarding Apply Cancel

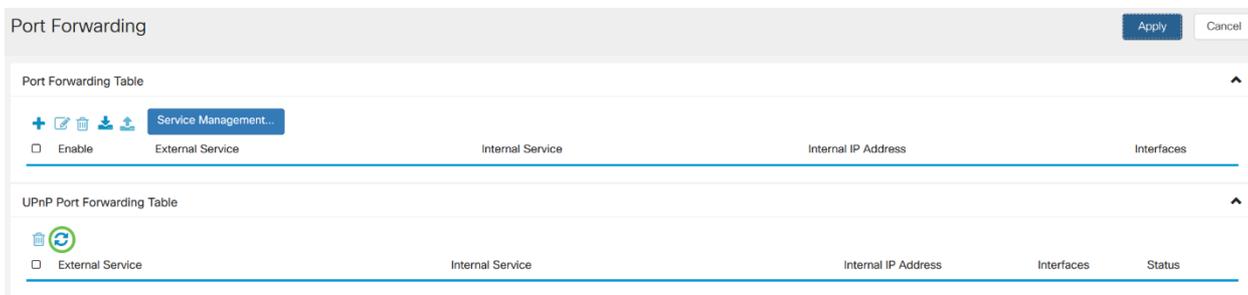
Port Forwarding Table Service Management...

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

UPnP Port Forwarding Table

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

Passaggio 7. Nella tabella di inoltro porta UPnP (Universal Plug and Play), fare clic sull'icona di **aggiornamento** per aggiornare i dati. Le regole di inoltro della porta per UPnP vengono aggiunte dinamicamente dall'applicazione UPnP.



Configura attivazione porta

Per configurare l'attivazione delle porte, attenersi alla seguente procedura:

Passaggio 1. Accedere all'utility di configurazione Web. Immettere il nome utente e la password per il router e fare clic su **Login**. Il nome utente e la password predefiniti sono *cisco*.



Router

Username **1**

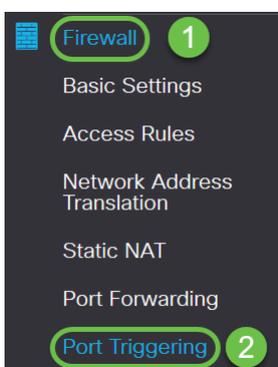
Password **2**

English **3**

Login **3**

In questo articolo, utilizzeremo la RV260 per configurare l'attivazione delle porte. La configurazione può variare a seconda del modello utilizzato.

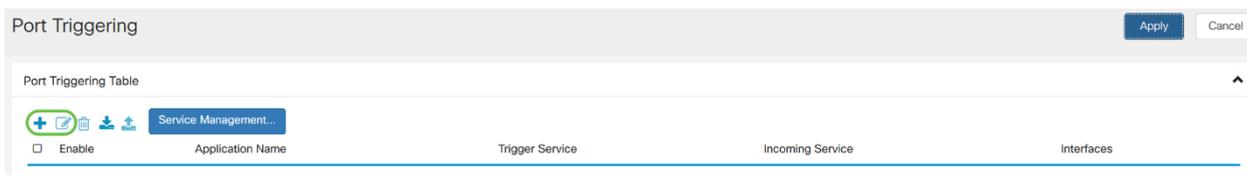
Passaggio 2. Fare clic su **Firewall > Port Triggering**.



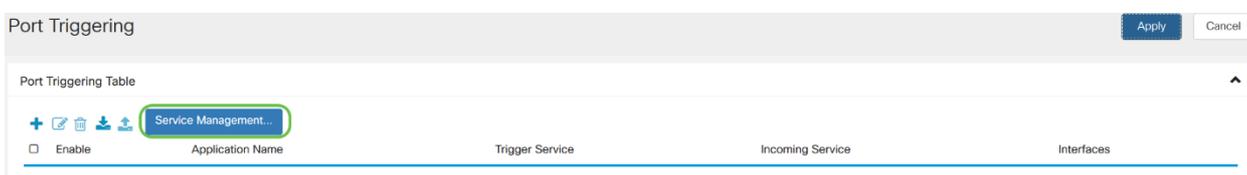
Passaggio 3. Per aggiungere o modificare un servizio nella tabella di attivazione della porta, configurare quanto segue:

Fare clic su **Icona Aggiungi** oppure selezionare la riga e fare clic su **Icona Modifica** e immettere le informazioni:

Attiva	Selezionare per abilitare l'attivazione della porta
Nome applicazione	Immettere il nome dell'applicazione
Servizio trigger	Selezionare un servizio dall'elenco a discesa. Se un servizio non è presente nell'elenco, è possibile aggiungerlo o modificarlo seguendo le istruzioni nella sezione Gestione dei servizi.
Servizio in ingresso	Selezionare un servizio dall'elenco a discesa. Se un servizio non è presente nell'elenco, è possibile aggiungerlo o modificarlo seguendo le istruzioni nella sezione Gestione dei servizi.
Interfacce	Selezionare l'interfaccia dall'elenco a discesa



Passaggio 4. Fare clic su **Service Management** per aggiungere o modificare una voce nella lista dei servizi.



Passaggio 5. In *Service Management*, fare clic su **add icon** o selezionare la riga e fare clic su **edit icon**.

Configurare quanto segue:

Nome applicazione: nome del servizio o dell'applicazione.

Protocollo - Protocollo richiesto. Fare riferimento alla documentazione del servizio che si sta ospitando.

Port Start/ICMP Type/IP Protocol: intervallo di numeri di porta riservati per questo servizio.

Port End: ultimo numero della porta riservata per il servizio.

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	--

Per aggiungere un servizio, fare clic sull'icona con il segno più e configurare Nome, Protocollo, Porta Start/ICMP Tipo/Protocollo IP e Porta End/Codice ICMP.

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

Per modificare un servizio, selezionare una riga e fare clic sull'icona Modifica per configurare i campi come mostrato di seguito.

