Configurazione dell'inoltro porte/trigger porte/NAT sui router serie RV34x

Obiettivo

Spiegare lo scopo dell'inoltro e dell'attivazione delle porte e fornire istruzioni per configurare queste funzionalità sui router serie RV34x.

- Confronto tra inoltro e attivazione delle porte
- Impostazione dell'inoltro e dell'attivazione delle porte
- Configurazione di Network Address Translation (NAT)

Dispositivi interessati

- Serie RV34x Router

Versione del software

- 1.0.01.17

Confronto tra inoltro e attivazione delle porte

Queste funzionalità consentono ad alcuni utenti Internet di accedere a risorse specifiche della rete, proteggendo al contempo le risorse che si desidera mantenere private. Alcuni esempi di utilizzo di questa funzionalità: hosting di server Web/e-mail, sistemi di allarme e videocamere di sicurezza (per inviare il video a un computer fuori sede). L'inoltro porte apre le porte in risposta al traffico in entrata per un servizio specificato.

Una lista di queste porte e la relativa descrizione vengono impostate quando si immettono le informazioni nella sezione Service Management della procedura guidata di configurazione. Quando si configurano queste porte, non è possibile utilizzare lo stesso numero di porta sia per l'inoltro che per l'attivazione.

Port Forwarding

L'inoltro delle porte è una tecnologia che consente l'accesso pubblico ai servizi sui dispositivi di rete sulla LAN (Local Area Network) tramite l'apertura di una porta specifica per un servizio in risposta al traffico in entrata. In questo modo, i pacchetti hanno un percorso chiaro verso la destinazione desiderata, che consente velocità di download più elevate e latenza ridotta. È impostato per un singolo computer della rete. È necessario aggiungere l'indirizzo IP del computer specifico, che non può essere modificato.

Si tratta di un'operazione statica che apre un intervallo specifico di porte selezionate e non viene modificata. Ciò potrebbe aumentare i rischi per la sicurezza poiché le porte configurate sono sempre aperte.

Si immagini che una porta sia sempre aperta sulla porta al dispositivo assegnato.

Port-trigger

L'attivazione delle porte è simile all'inoltro delle porte, ma un po' più sicura. La differenza è che la porta di attivazione non è sempre aperta per il traffico specifico. Dopo che una risorsa della LAN invia il traffico in uscita tramite una porta di attivazione, il router rimane in ascolto del traffico in entrata tramite una porta o un intervallo di porte specificato. Le porte attivate vengono chiuse in assenza di attività, il che aumenta la sicurezza. Un altro vantaggio è che più computer della rete possono accedere a questa porta in momenti diversi. Pertanto, non è necessario conoscere l'indirizzo IP del computer che lo attiverà in anticipo, lo fa automaticamente.

Pensate di dare un lasciapassare a qualcuno, ma c'è un portiere lì che controlla il vostro lasciapassare ogni volta che entrate e poi chiude la porta fino a quando arriva la persona successiva con un lasciapassare.

Impostazione dell'inoltro e dell'attivazione delle porte

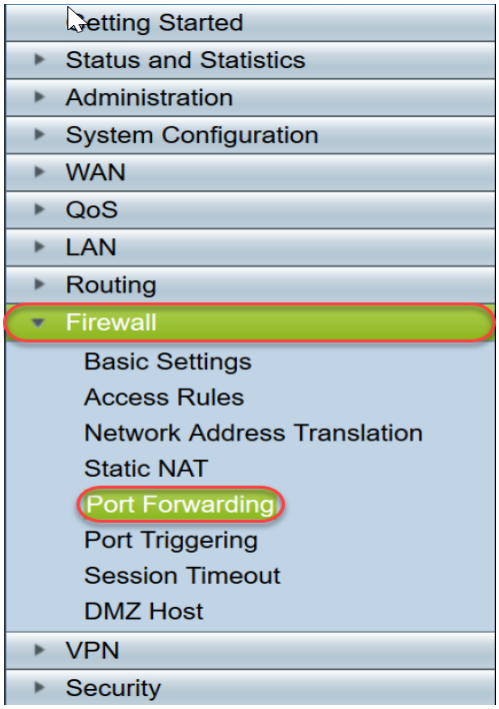
Port Forwarding

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

Passaggio 1. Accedere all'utility di configurazione Web. Immettere l'indirizzo IP del router nella barra di ricerca/indirizzo. È possibile che il browser invii un avviso per segnalare che il sito Web non è attendibile. Accedere al sito Web. Per ulteriori informazioni su questo passaggio, fare clic qui.

Immettere il nome utente e la password per il router e fare clic su **Log In** (Accedi). Il nome utente e la password predefiniti sono cisco.

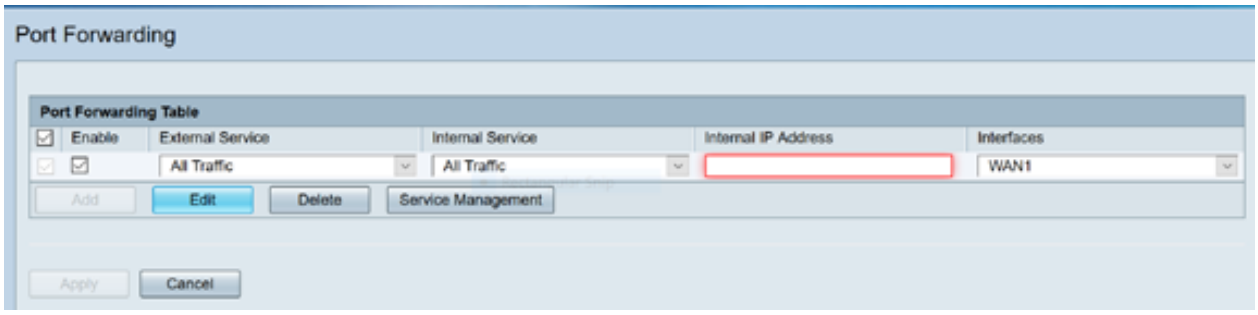
2. Dal menu principale sul lato sinistro, **fare clic su Firewall > Port Forwarding**



Nella tabella Inoltro porte, fare clic su **Add** o selezionare la riga e fare clic su **Edit** per configurare quanto segue:

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 nella 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 nella sezione Gestione servizi.
Indirizzo IP interno	Immettere gli indirizzi IP interni del server.
Interfacce	Selezionare l'interfaccia dall'elenco a discesa per applicare l'inoltro delle porte.
Stato	Abilita o disabilita la regola di inoltro della porta.

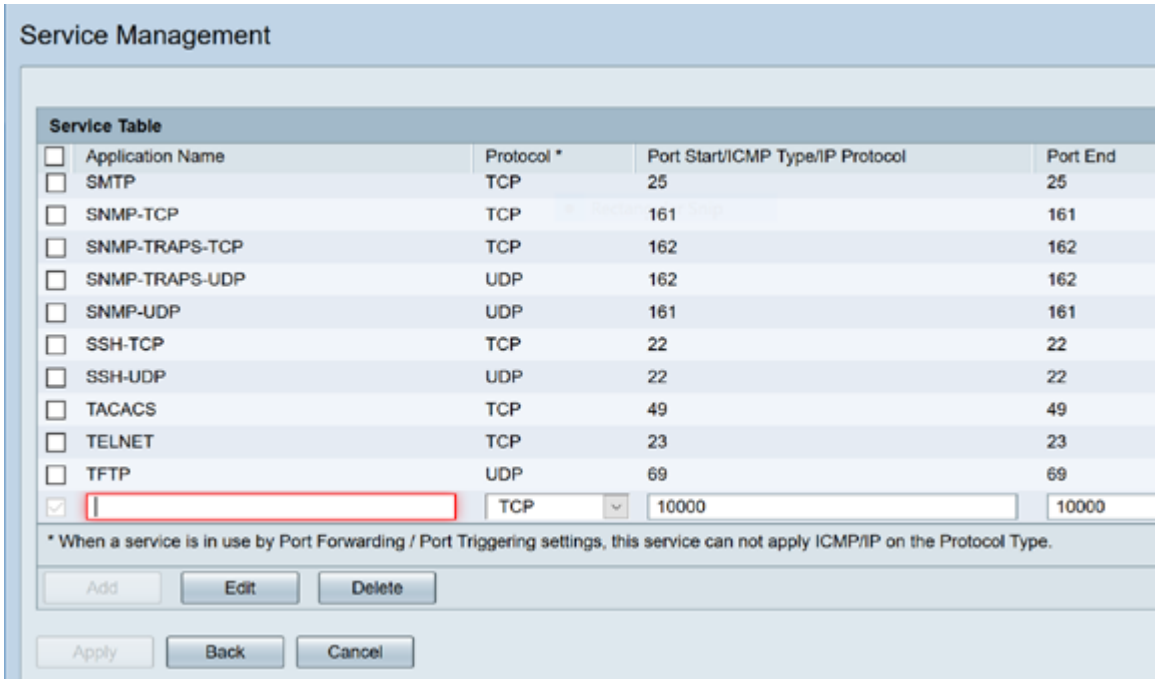


Ad esempio, un'azienda ospita un server Web (con un indirizzo IP interno di 192.0.2.1) sulla propria rete LAN. Impossibile abilitare una regola di inoltro porta per il traffico HTTP. In tal modo, si consentirebbero le richieste provenienti da Internet in tale rete. La società imposta il numero di porta 80 (HTTP) per l'inoltro all'indirizzo IP 192.0.2.1, quindi tutte le richieste HTTP provenienti da utenti esterni verranno inoltrate a 192.0.2.1. È impostato per il dispositivo specifico nella rete.

Passaggio 3. Fare clic su **Gestione servizio**

Nella tabella dei servizi, fare clic su **Aggiungi** o selezionare una riga e fare clic su **Modifica** e configurare quanto segue:

- Nome applicazione - Nome del servizio o dell'applicazione
- Protocollo: protocollo obbligatorio. 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
- Fine porta - Ultimo numero della porta, riservato per questo servizio

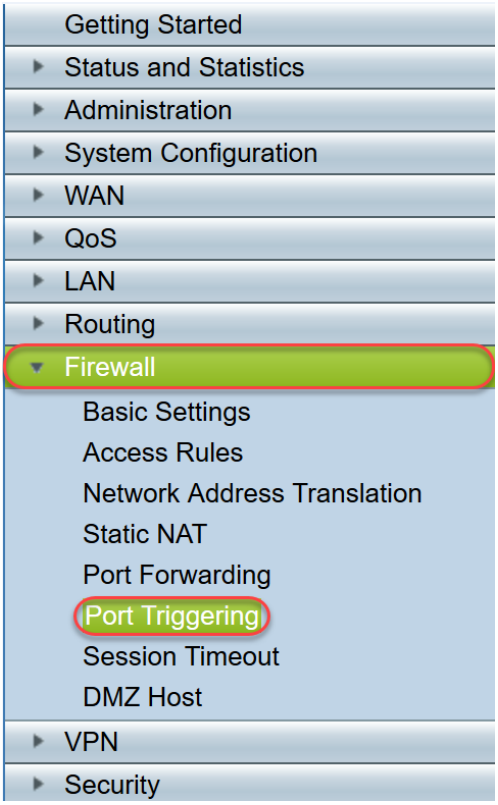


Passaggio 4. Fare clic su **Applica**

Port-trigger

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

Passaggio 1. Accedere all'utility di configurazione Web**. Dal menu principale sul lato sinistro, fare clic su Firewall > Port Triggering**

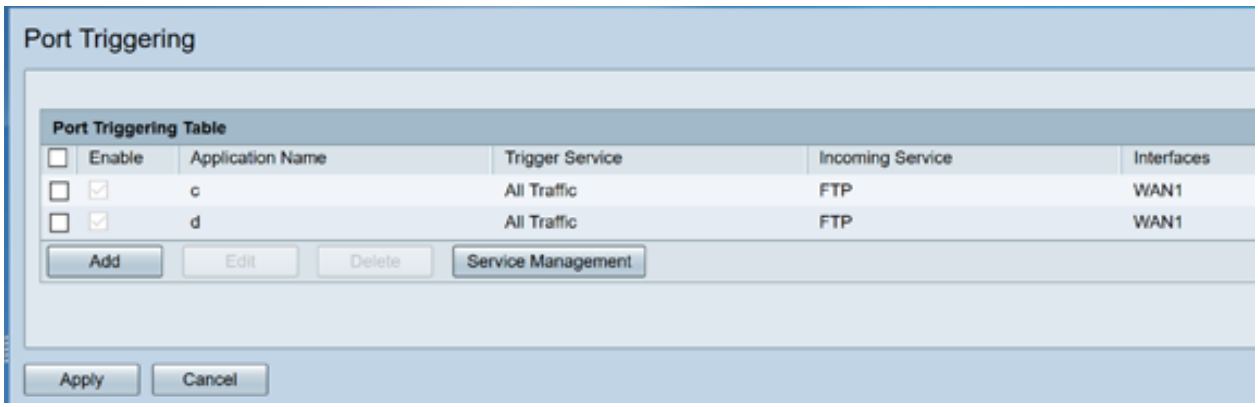


Passaggio 2. Per aggiungere o modificare un servizio nella tabella di attivazione della porta, configurare quanto segue:

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 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 servizi.
Interfacce	Selezionare l'interfaccia dall'elenco a discesa.
Stato	Abilitare o disabilitare la regola di attivazione della porta.

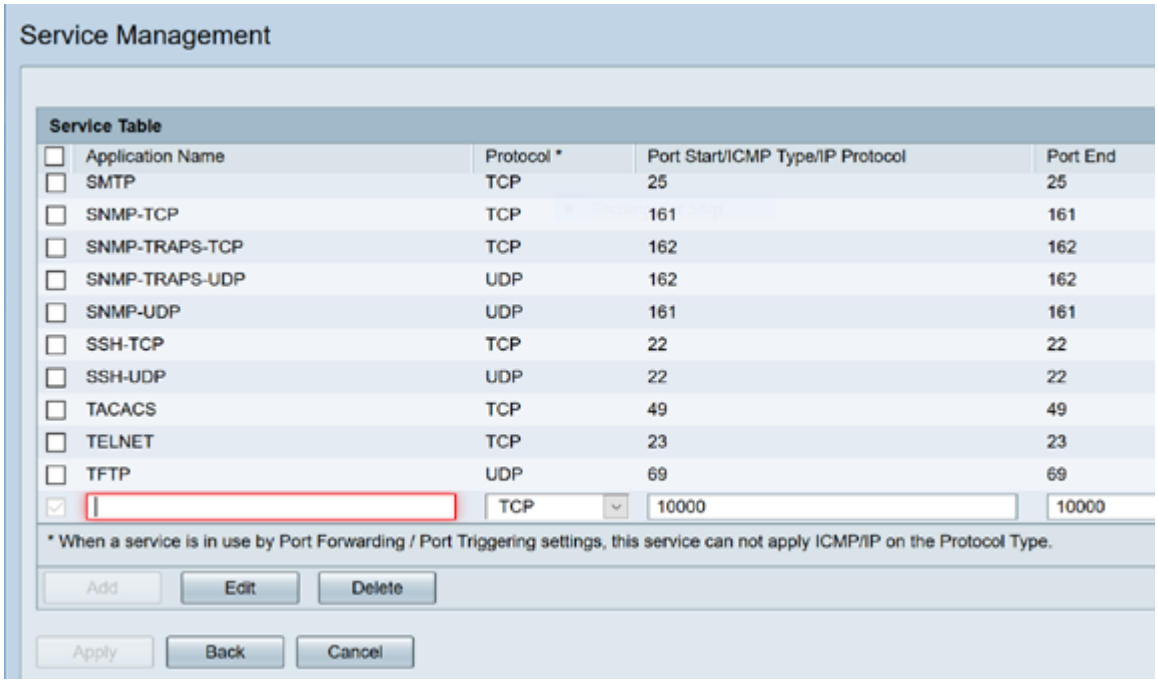
Fare clic su **Aggiungi** (o selezionare la riga e fare clic su **Modifica**) e immettere le informazioni seguenti:



Passaggio 3. Fare clic su **Gestione servizi** per aggiungere o modificare una voce nella lista dei servizi.

Nella tabella dei servizi, fare clic su **Add** o **Edit** e configurare quanto segue:

- Nome applicazione - Nome del servizio o dell'applicazione
- Protocollo: protocollo obbligatorio. 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
- Fine porta - Ultimo numero della porta, riservato per questo servizio



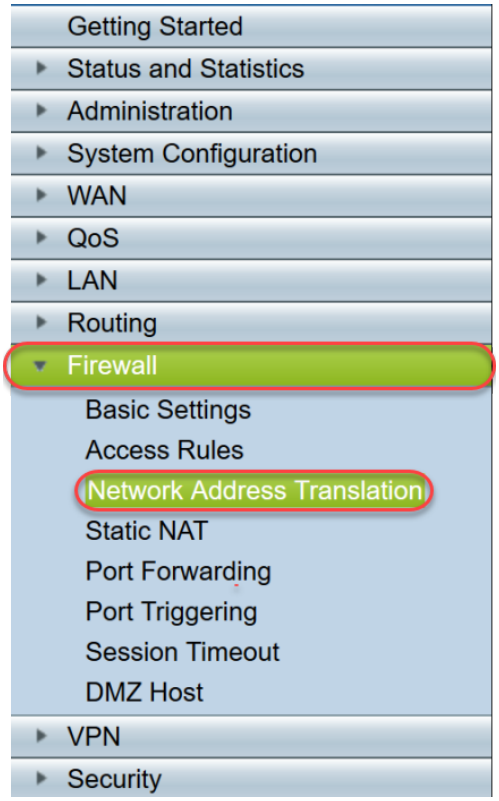
Passaggio 4. Fare clic su **Applica**

Network Address Translation

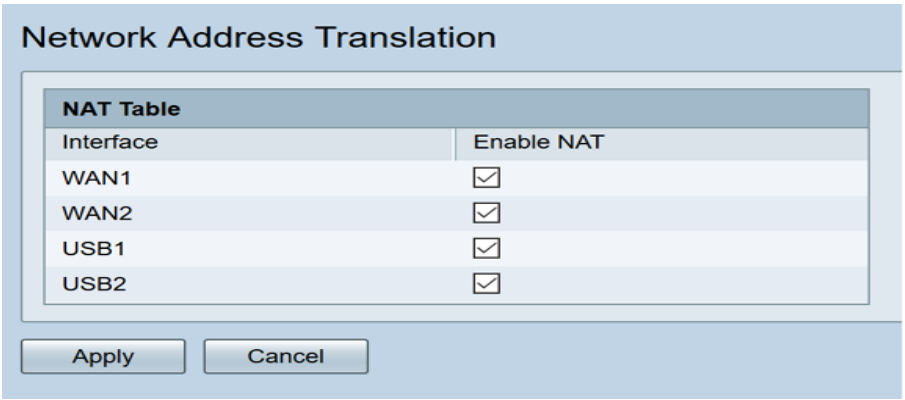
NAT (Network Address Translation) consente alle reti IP private con indirizzi IP non registrati di connettersi alla rete pubblica. Si tratta di un protocollo comunemente configurato nella maggior parte delle reti. NAT converte gli indirizzi IP privati della rete interna in indirizzi IP pubblici prima che i pacchetti vengano inoltrati alla rete pubblica. Ciò consente a un gran numero di host su una rete interna di accedere a Internet attraverso un numero limitato di indirizzi IP pubblici. Ciò contribuisce anche a proteggere gli indirizzi IP privati da attacchi dannosi o da rilevamenti, in quanto gli indirizzi IP privati vengono nascosti.

Per configurare NAT, eseguire la procedura seguente

Passaggio 1. Fare clic su **Firewall> Network Address Translation**



Passaggio 2. Nella tabella NAT, selezionare Abilita NAT per ciascuna interfaccia applicabile nell'elenco per abilitare



Passaggio 3. Fare clic su **Applica**

Port forwarding, Port Triggering e NAT sono stati configurati correttamente.

Altre risorse

- Per la configurazione di NAT statico, fare clic qui
- Per le risposte a molte domande sui router, compresa la serie RV3xx, fare clic qui
- Per le domande frequenti sulla serie RV34x, fare clic qui
- Per ulteriori informazioni su RV345 e RV345P, fare clic qui
- Per ulteriori informazioni sulla configurazione di Service Management sulla serie RV34x, fare clic qui

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco