Aggiunta e configurazione delle regole di accesso su RV130 e RV130W

Obiettivo

I dispositivi di rete offrono funzionalità di base di filtro del traffico con regole di accesso. Una regola di accesso è una singola voce di un elenco di controllo di accesso (ACL, Access Control List) che specifica una regola di autorizzazione o rifiuto (per inoltrare o eliminare un pacchetto) basata sul protocollo, un indirizzo IP di origine e destinazione o una configurazione di rete.

L'obiettivo di questo documento è mostrare come aggiungere e configurare una regola di accesso sugli RV130 e RV130W.

Dispositivi interessati

RV130

RV130W

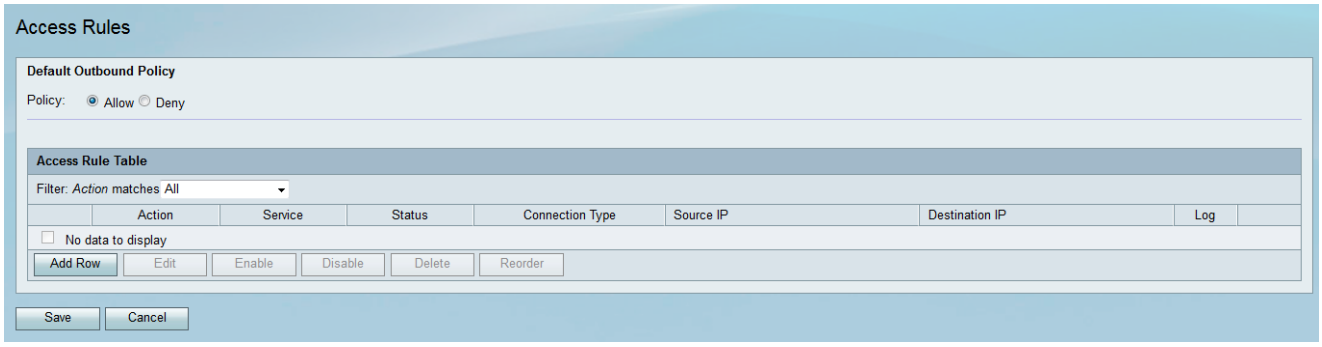
Versioni software

·Versione 1.0.1.3

Aggiungere e configurare una regola di accesso

Impostazione dei criteri predefiniti in uscita

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Firewall > Regole di accesso**. Viene visualizzata la pagina *Regole di accesso*:



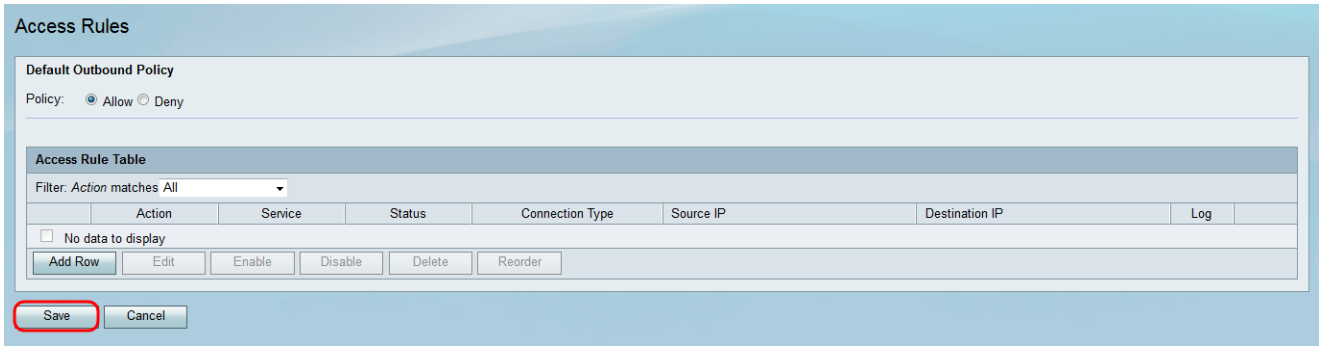
Passaggio 2. Nell'area *Criterio predefinito uscita* fare clic sul pulsante di opzione desiderato per scegliere un criterio per il traffico in uscita. Il criterio viene applicato ogni volta che non sono configurate regole di accesso o criteri di accesso a Internet. L'impostazione predefinita è **Allow** (Consenti), che consente il passaggio di tutto il traffico diretto a Internet.

Le opzioni disponibili sono definite come segue:

·Consenti: consente tutti i tipi di traffico dalla LAN a Internet.

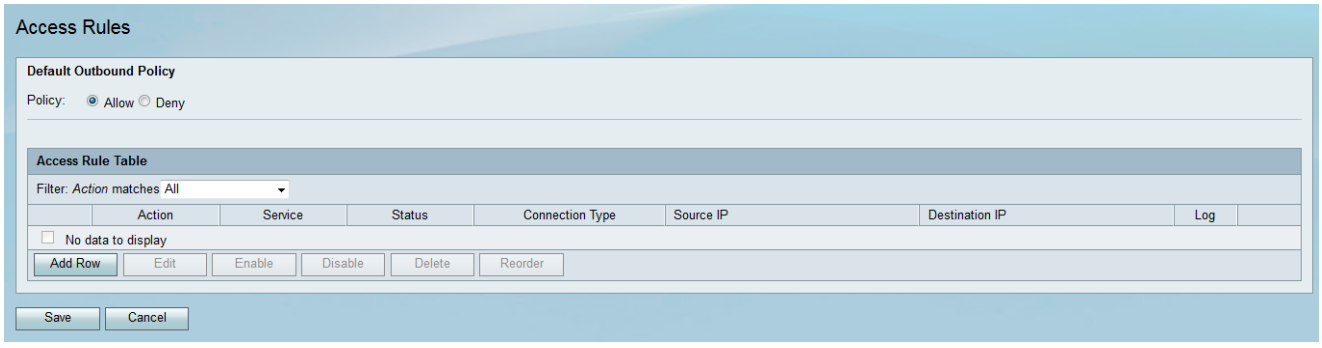
·Nega: blocca tutti i tipi di traffico in uscita dalla LAN verso Internet.

Passaggio 3. Fare clic su **Save** per salvare le impostazioni.

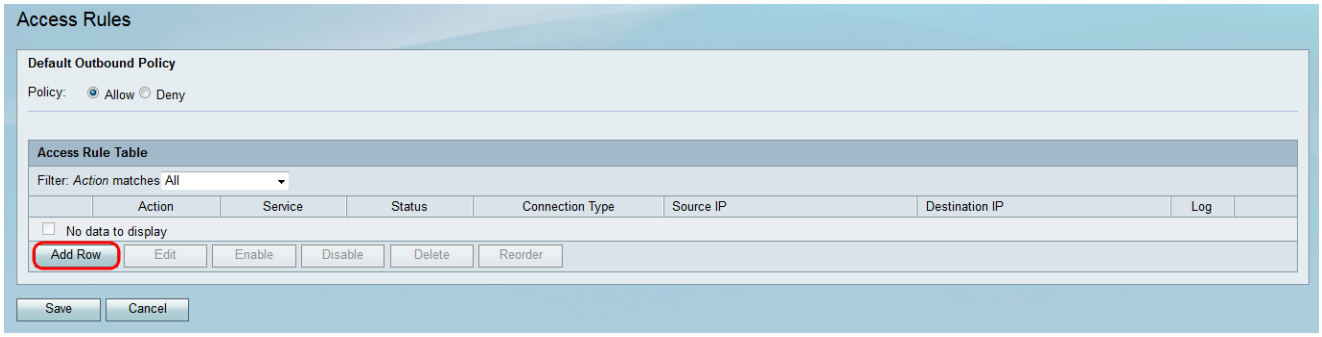


Aggiunta di una regola di accesso

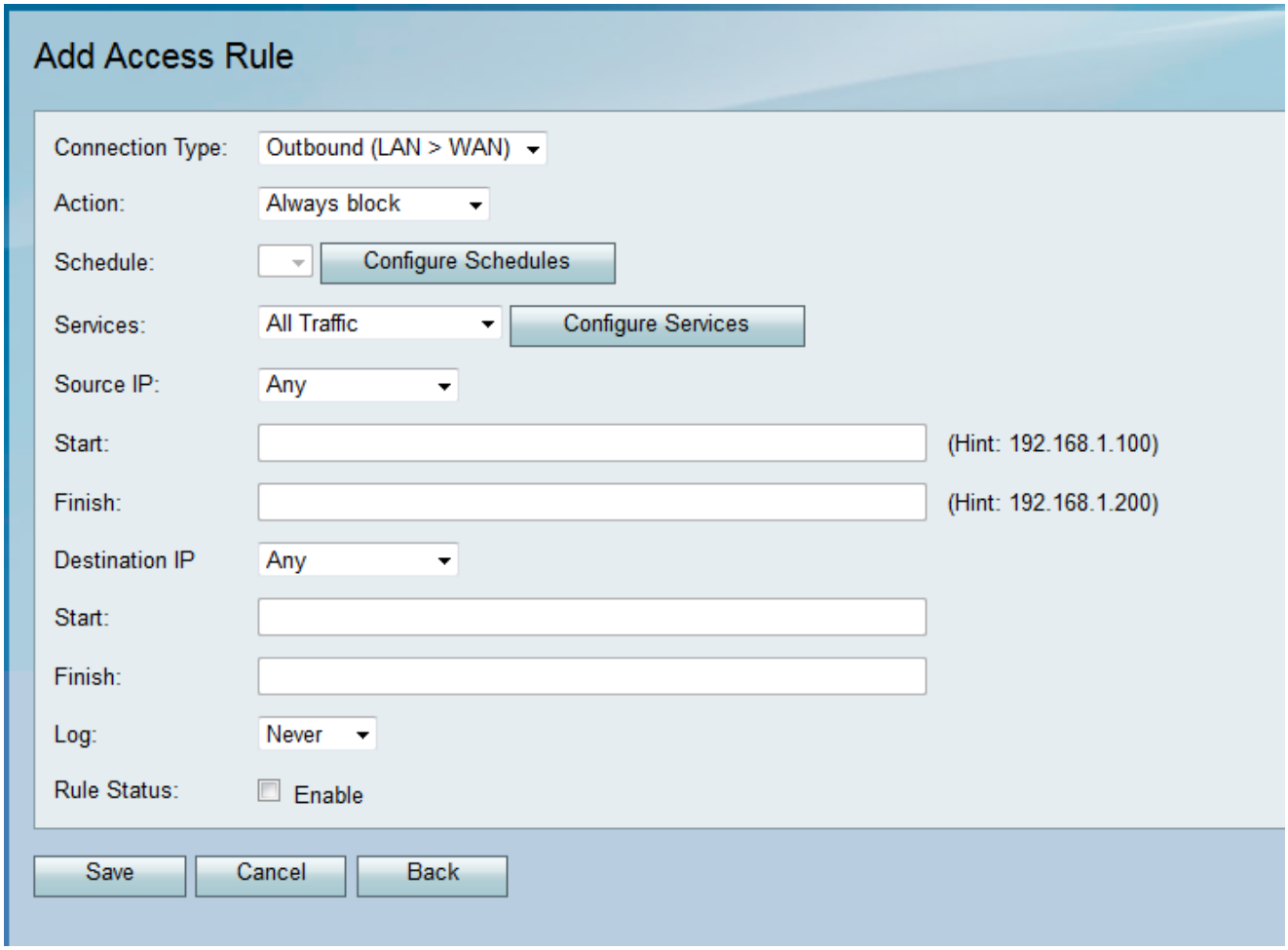
Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Firewall > Regole di accesso**. Viene visualizzata la finestra *Regole di accesso*:



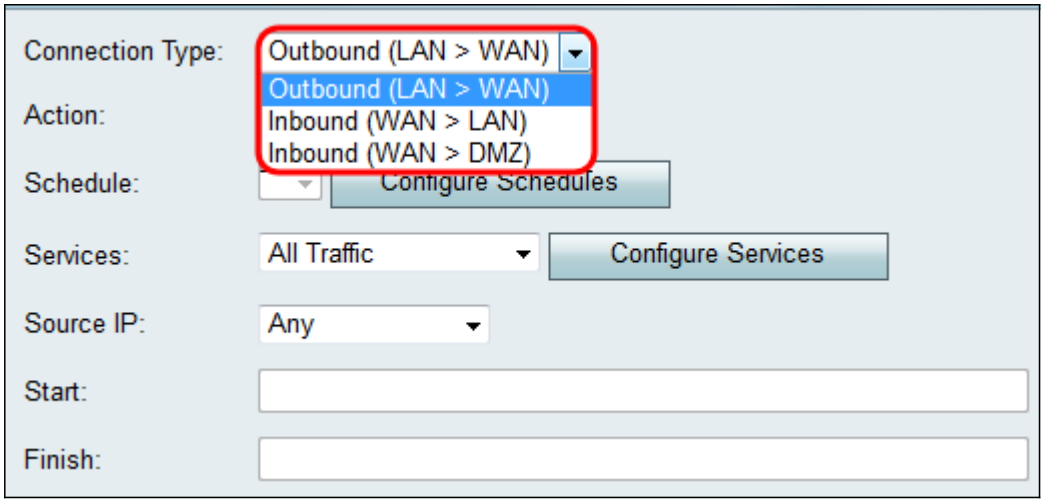
Passaggio 2. Fare clic su **Aggiungi riga** nella *tabella Regole di accesso* per aggiungere una nuova regola di accesso.



Viene visualizzata la pagina *Aggiungi regola di accesso*:



Passaggio 3. Dall'elenco a discesa *Tipo di connessione*, scegliere il tipo di traffico a cui applicare la regola.



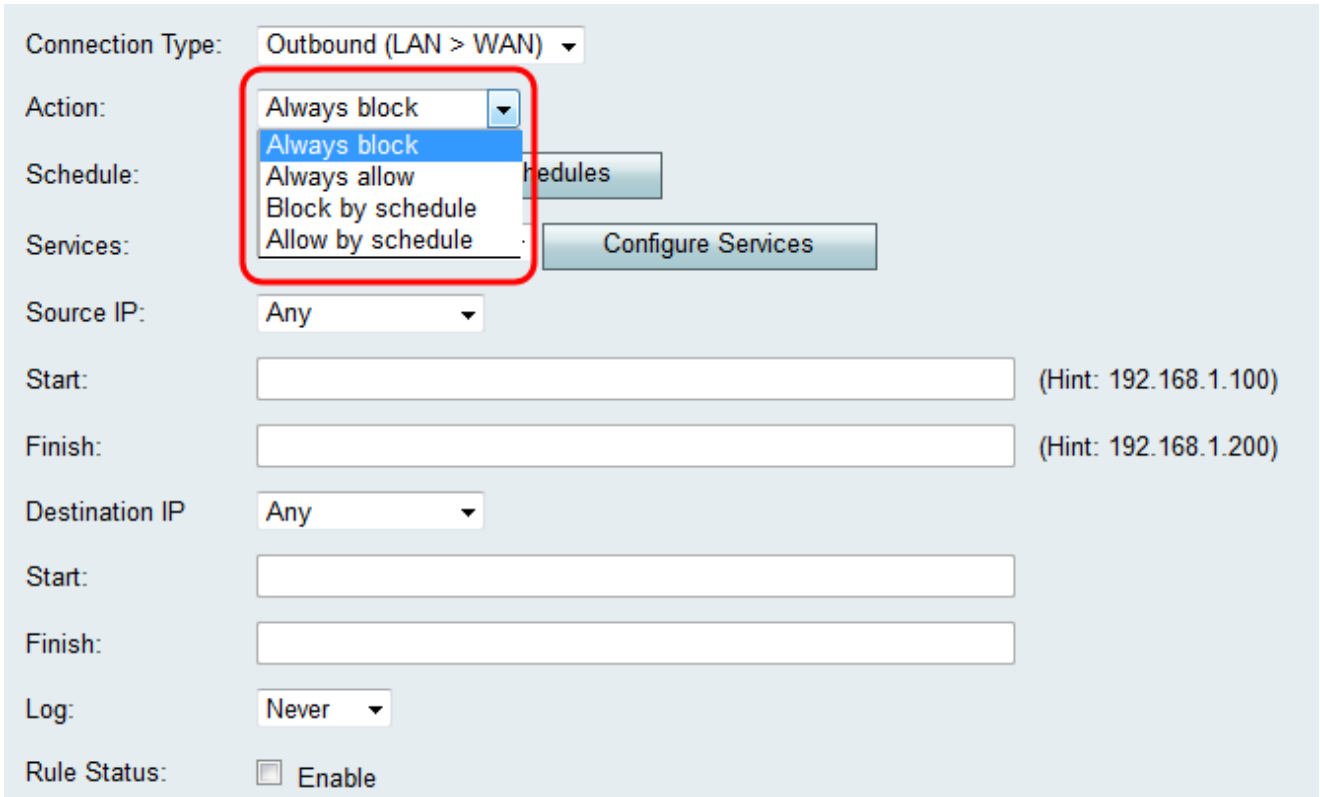
Le opzioni disponibili sono definite come segue:

·In uscita (LAN > WAN): la regola influenza i pacchetti provenienti dalla rete locale (LAN) e che vanno su Internet (WAN).

·In entrata (WAN > LAN): la regola interessa i pacchetti provenienti da Internet (WAN) e che vanno alla rete locale (LAN).

·In entrata (WAN > DMZ): la regola influenza i pacchetti provenienti da Internet (WAN) e che vanno nella sottorete della zona demilitarizzata (DMZ).

Passaggio 4. Dall'elenco a discesa *Azione*, scegliere l'azione da eseguire quando una regola viene confrontata.



Le opzioni disponibili sono definite come segue:

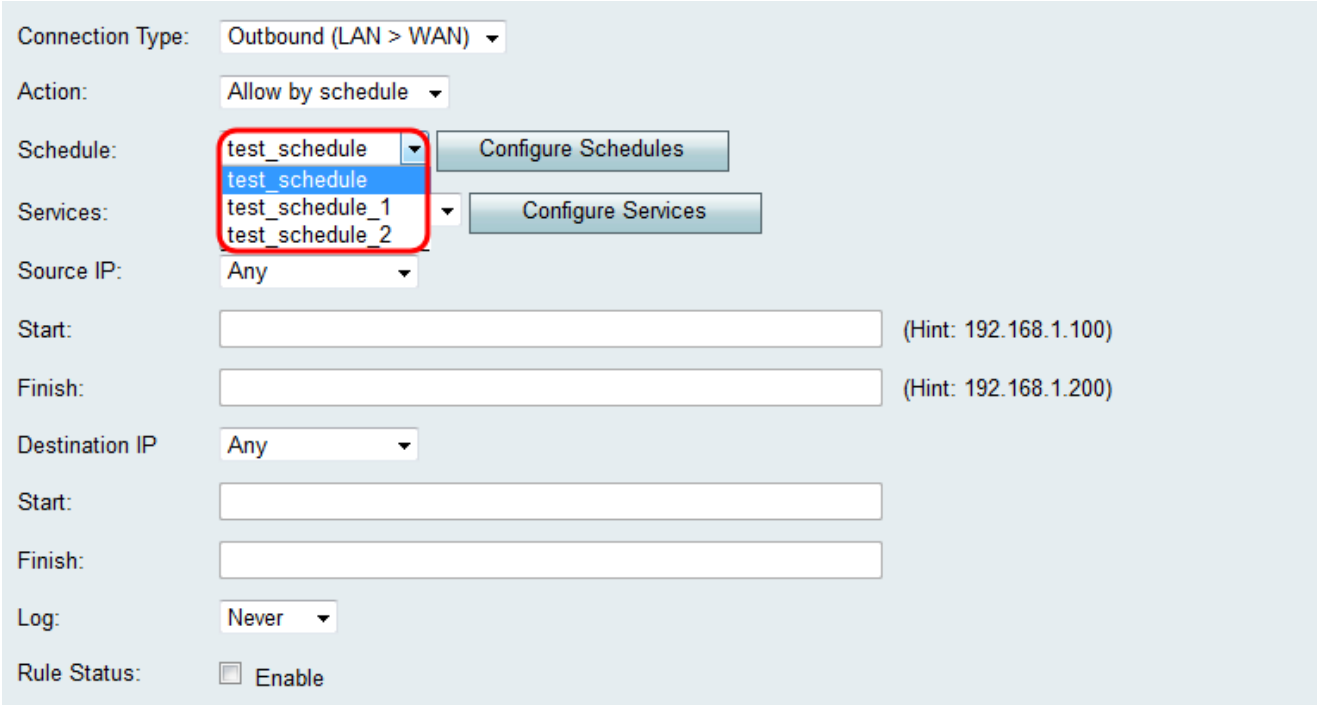
·Blocca sempre: nega sempre l'accesso se vengono soddisfatte le condizioni. Andare al passo 6.

·Consenti sempre — Consenti sempre l'accesso se le condizioni vengono soddisfatte. Andare al passo 6.

·Blocca in base alla pianificazione: nega l'accesso se le condizioni vengono soddisfatte durante una pianificazione preconfigurata.

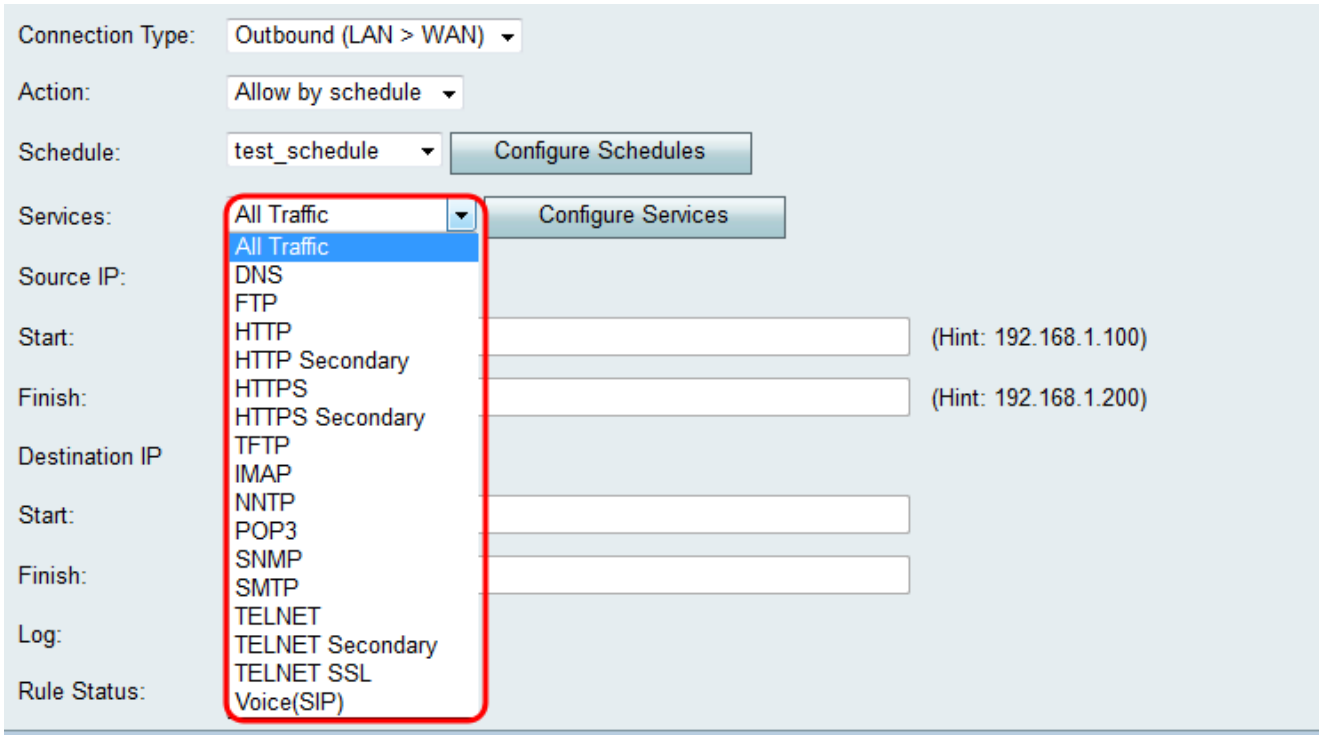
·Consenti in base alla pianificazione: consente l'accesso se le condizioni vengono soddisfatte durante una pianificazione preconfigurata.

Passo 5: se si sceglie **Blocca per programma** o **Consenti per programma** nel Passo 4, scegliere il programma appropriato dall'elenco a discesa *Programma*.



Nota: Per creare o modificare una pianificazione, fare clic su Configura pianificazioni. Per ulteriori informazioni e linee guida, fare riferimento a *Configurazione delle pianificazioni su RV130 e RV130W*.

Passaggio 6. Scegliere il tipo di servizio a cui si applica la regola di accesso dall'elenco a discesa *Services*.



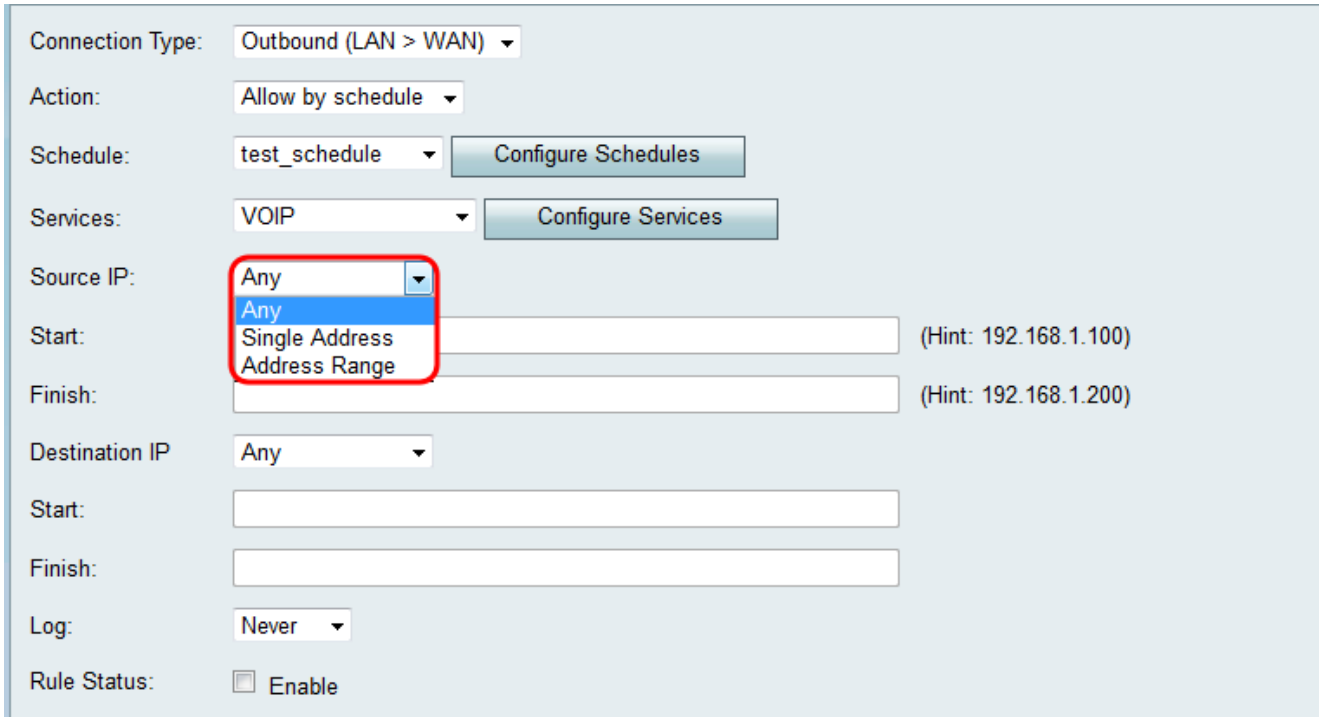
Nota: Per aggiungere o modificare un servizio, fare clic su Configura servizi. Per ulteriori informazioni e linee guida, consultare il documento sulla *configurazione della gestione dei servizi sugli switch RV130 e RV130W*.

Configurazione degli indirizzi IP di origine e destinazione per il traffico in uscita

Attenersi alla procedura descritta in questa sezione se è stato selezionato **In uscita (LAN > WAN)** come Tipo di connessione nel passo 3 di *Aggiunta di una regola di accesso.*

Nota: Se nel Passaggio 3 di Aggiunta di una regola di accesso è stato selezionato un tipo di connessione in entrata, passare alla sezione successiva: *Configurazione degli indirizzi IP di origine e destinazione per il traffico in entrata*.

Passaggio 1. Scegliere la modalità di definizione dell'indirizzo IP di origine dall'elenco a discesa *IP di origine*. Per il traffico in uscita, l'indirizzo IP di origine fa riferimento all'indirizzo o agli indirizzi (nella LAN) a cui verrebbe applicata la regola del firewall.



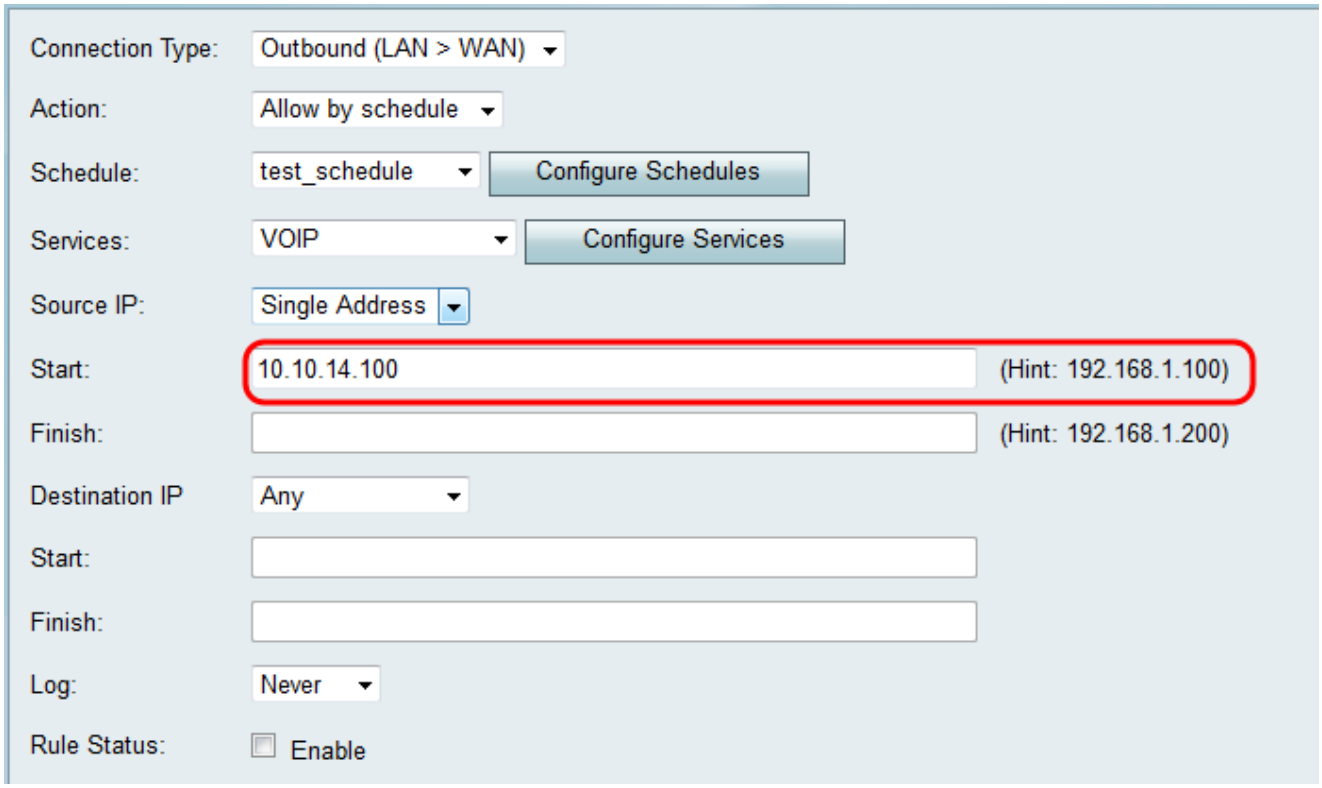
Le opzioni disponibili sono definite come segue:

·Any - Si applica al traffico proveniente da qualsiasi indirizzo IP nella rete locale. Lasciare pertanto vuoti i campi *Inizio* e *Fine*. Se si sceglie questa opzione, andare al passaggio 4.

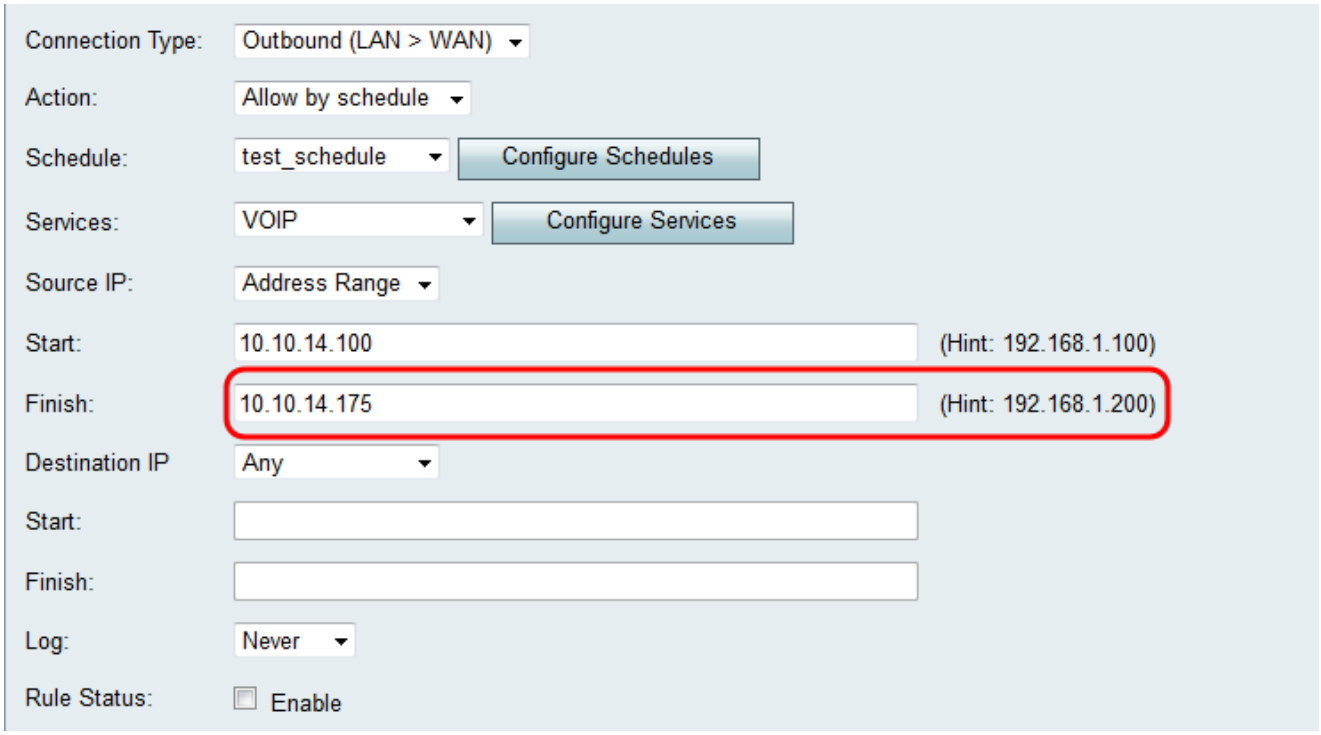
·Indirizzo singolo: si applica al traffico proveniente da un singolo indirizzo IP nella rete locale. Immettere l'indirizzo IP nel campo *Start*.

·Intervallo indirizzi: si applica al traffico proveniente da un intervallo di indirizzi IP nella rete locale. Per impostare l'intervallo, immettere l'indirizzo IP iniziale dell'intervallo nel campo *Inizio* e l'indirizzo IP finale nel campo *Fine*.

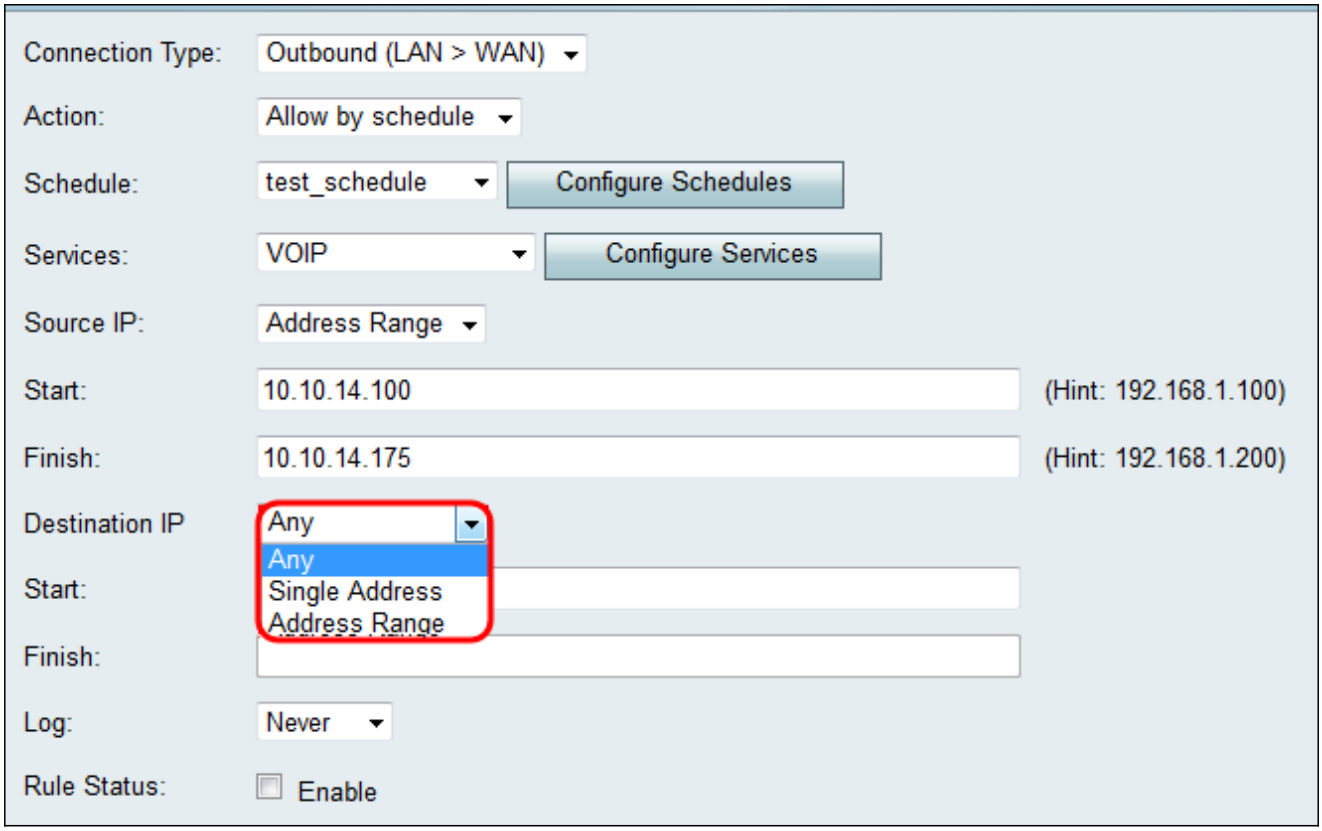
Passaggio 2. Se si sceglie **Indirizzo singolo** nel passaggio 1, immettere l'indirizzo IP che verrà applicato alla regola di accesso nel campo *Inizio*, quindi passare al passaggio 4. Se si sceglie **Intervallo di indirizzi** nel passaggio 1, immettere un indirizzo IP iniziale che verrà applicato alla regola di accesso nel campo *Inizio*.



Passaggio 3. Se si sceglie **Intervallo di indirizzi** al passaggio 1, immettere l'indirizzo IP finale che incapsulerà l'intervallo di indirizzi IP per la regola di accesso nel campo *Fine*.



Passaggio 4. Selezionare la modalità di definizione dell'IP di destinazione dall'elenco a discesa *IP di destinazione*. Per il traffico in uscita, l'indirizzo IP di destinazione si riferisce all'indirizzo o agli indirizzi (nella WAN) a cui viene autorizzato o rifiutato il traffico proveniente dalla rete locale.



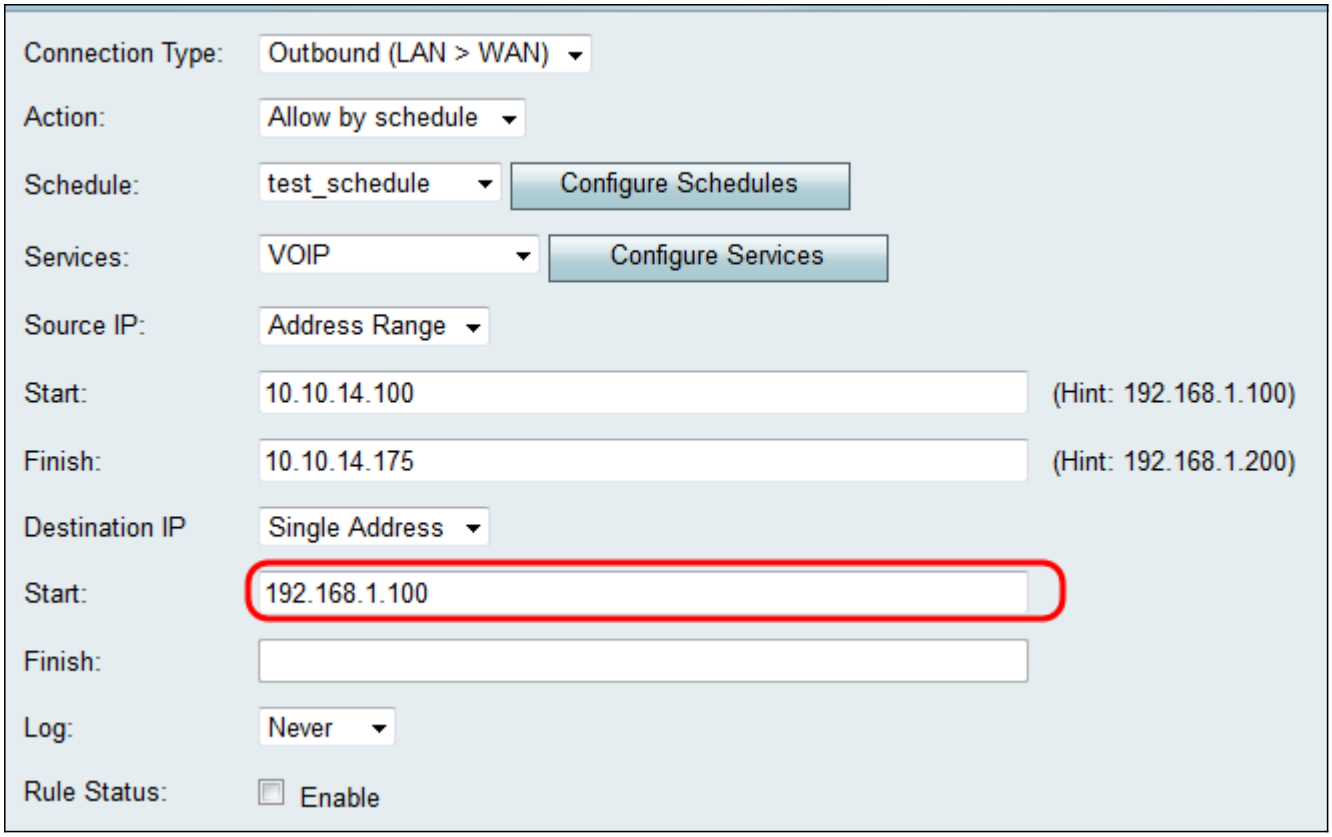
Le opzioni disponibili sono definite come segue:

·Any — Si applica al traffico diretto verso qualsiasi indirizzo IP nella rete Internet pubblica. Lasciare pertanto vuoti i campi *Inizio* e *Fine*.

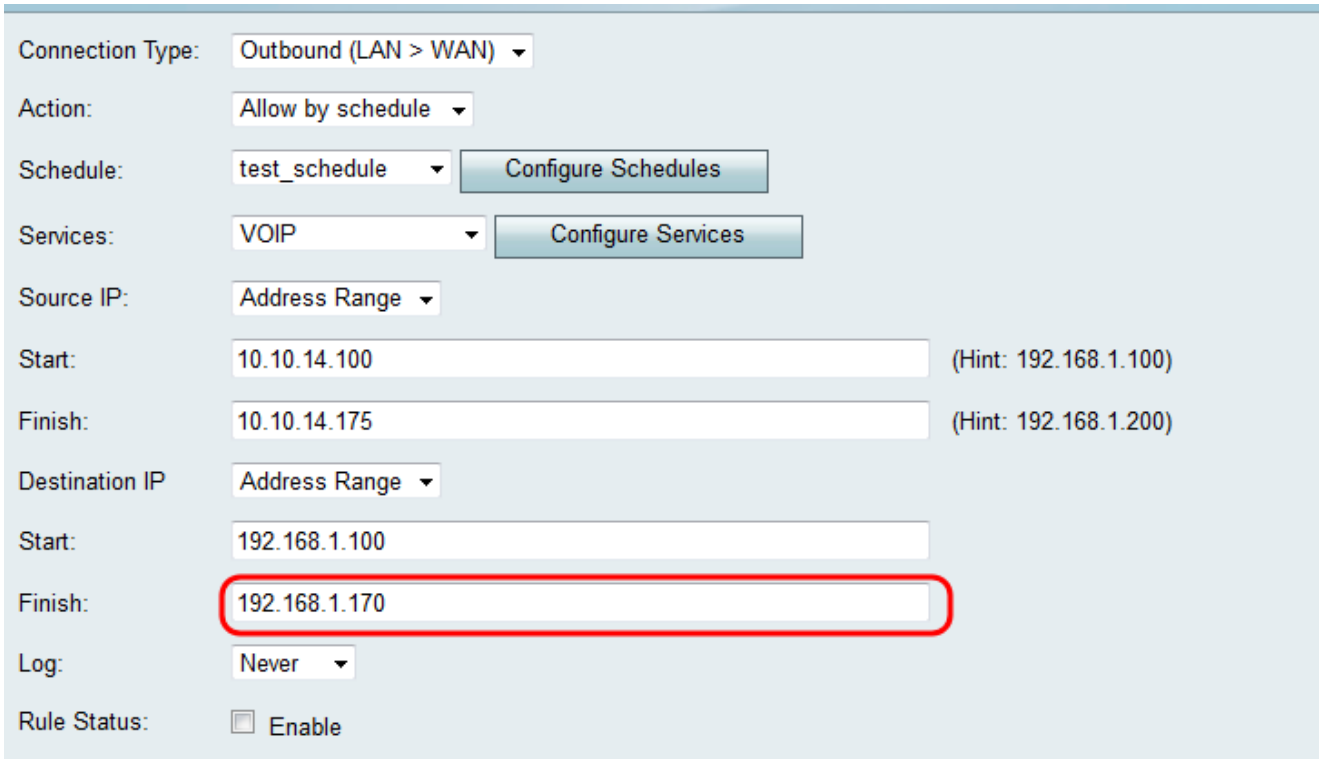
·Indirizzo singolo: si applica al traffico diretto verso un singolo indirizzo IP nella rete Internet pubblica. Immettere l'indirizzo IP nel campo *Start*.

·Intervallo indirizzi: si applica al traffico diretto verso un intervallo di indirizzi IP nell'Internet pubblica. Per impostare l'intervallo, immettere l'indirizzo IP iniziale dell'intervallo nel campo *Inizio* e l'indirizzo IP finale nel campo *Fine*.

Passaggio 5. Se si sceglie **Indirizzo singolo** al passaggio 4, immettere l'indirizzo IP che verrà applicato alla regola di accesso nel campo *Inizio*. Se si sceglie **Intervallo indirizzi** nel passaggio 4, immettere un indirizzo IP iniziale che verrà applicato alla regola di accesso nel campo *Inizio*.



Passaggio 6. Se si sceglie **Intervallo di indirizzi** al passaggio 4, immettere l'indirizzo IP finale che incapsulerà l'intervallo di indirizzi IP per la regola di accesso nel campo *Fine*.

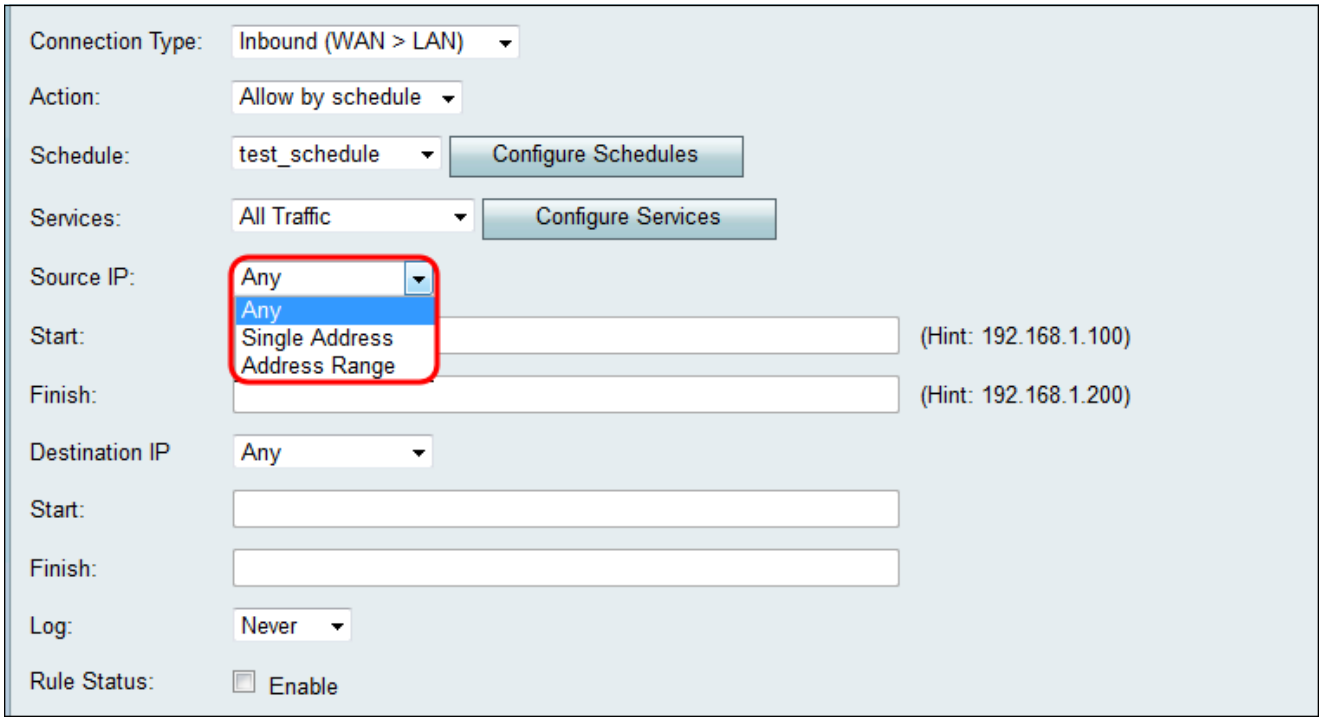


Configurazione degli indirizzi IP di origine e destinazione per il traffico in entrata

Seguire la procedura descritta in questa sezione se è stato selezionato **In entrata (WAN > LAN)** o **In entrata (WAN > DMZ)** come Tipo di connessione nel passo 3 di *Aggiunta di una regola di accesso*.

Passaggio 1. Scegliere la modalità di definizione dell'indirizzo IP di origine dall'elenco a

discesa *IP di origine*. Per il traffico in entrata, l'indirizzo IP di origine si riferisce all'indirizzo o agli indirizzi (nella WAN) a cui si applica la regola del firewall.



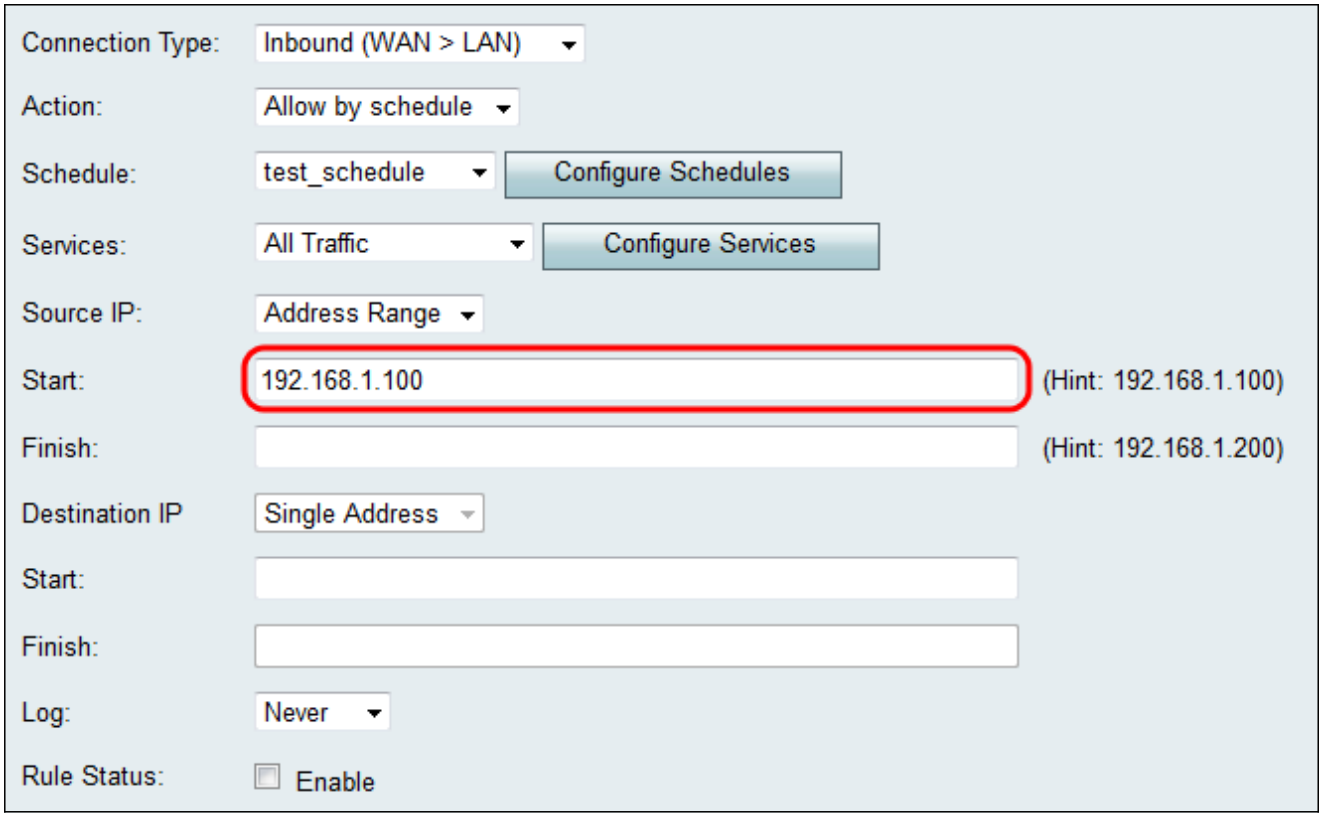
Le opzioni disponibili sono definite come segue:

·Any - Si applica al traffico proveniente da qualsiasi indirizzo IP nella rete Internet pubblica. Lasciare pertanto vuoti i campi *Inizio* e *Fine*. Se si sceglie questa opzione, andare al passaggio 4.

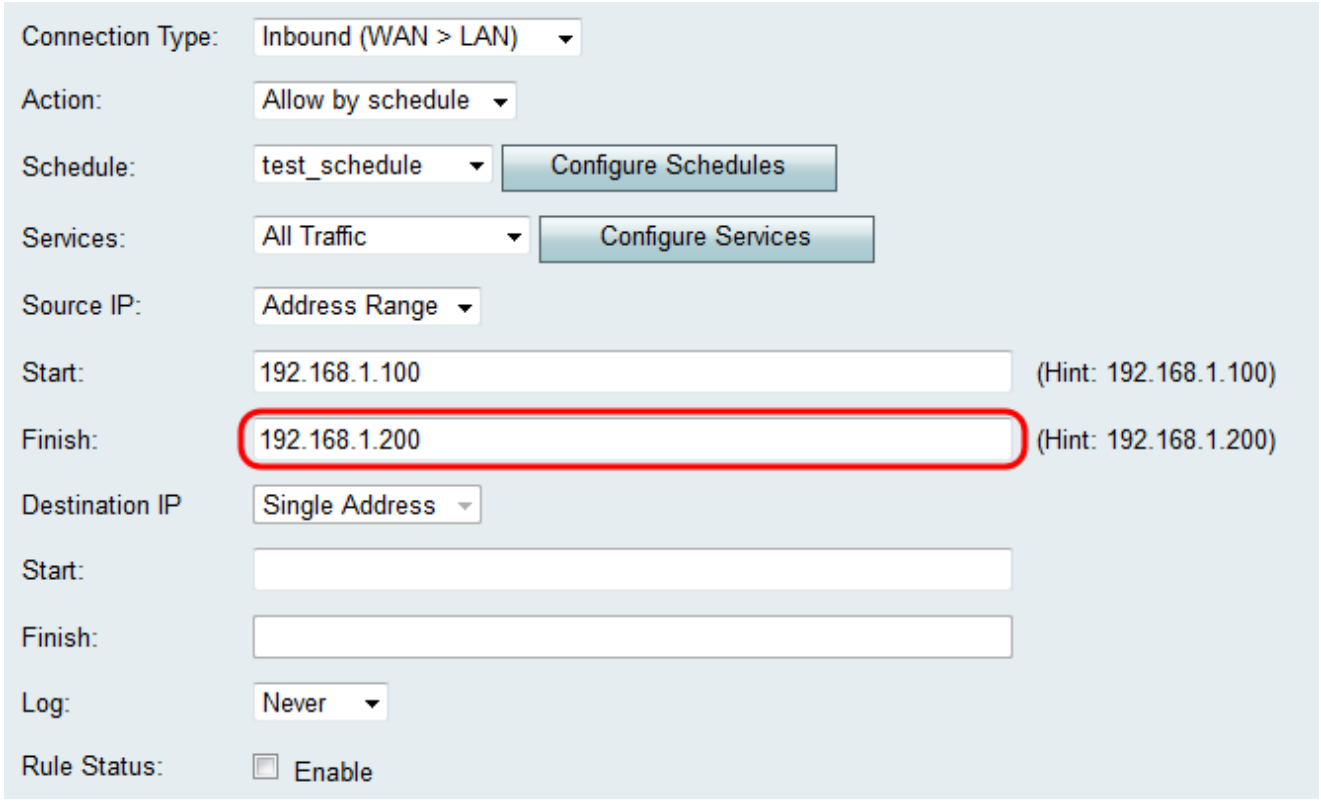
·Indirizzo singolo: si applica al traffico proveniente da un singolo indirizzo IP nella rete Internet pubblica. Immettere l'indirizzo IP nel campo *Start*.

·Intervallo di indirizzi: si applica al traffico proveniente da un intervallo di indirizzi IP nell'Internet pubblica. Per impostare l'intervallo, immettere l'indirizzo IP iniziale dell'intervallo nel campo *Inizio* e l'indirizzo IP finale nel campo *Fine*.

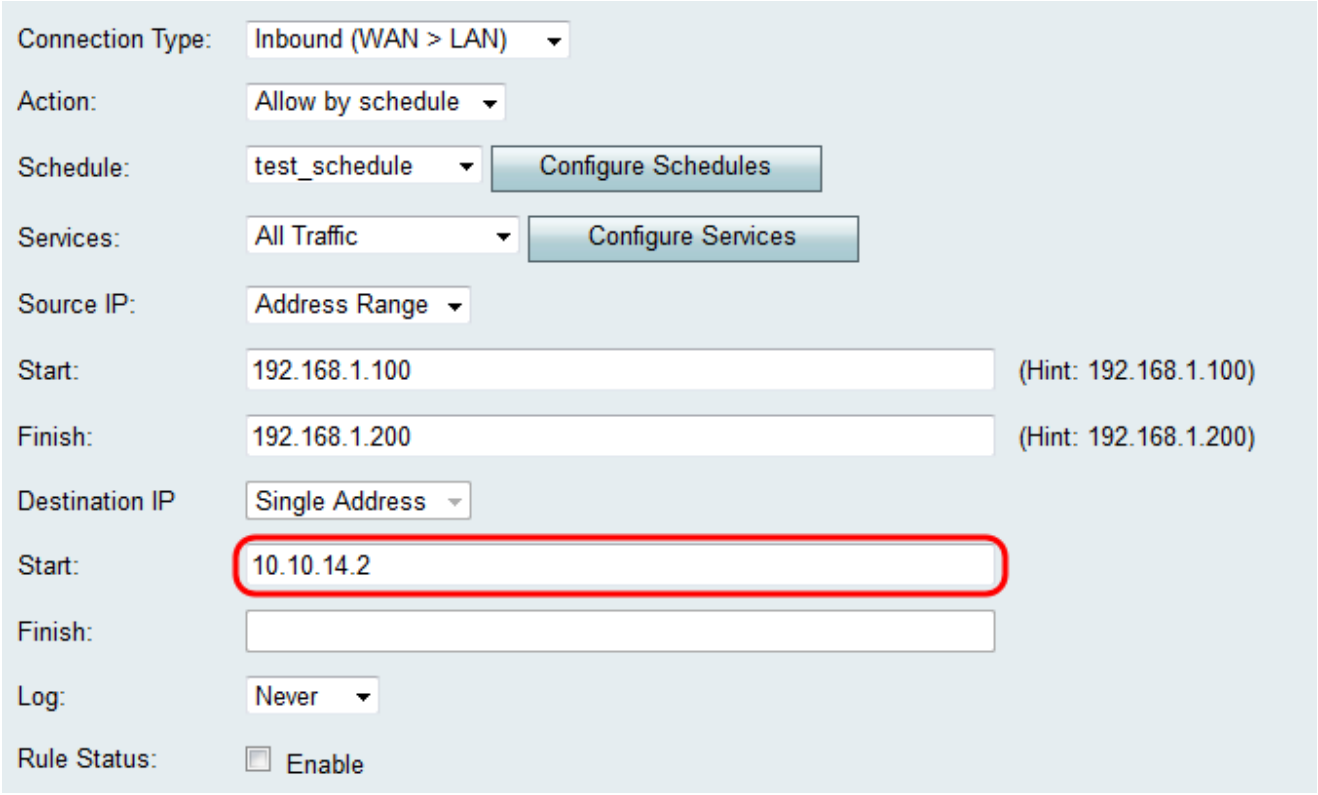
Passaggio 2. Se si sceglie **Indirizzo singolo** al passaggio 1, immettere l'indirizzo IP che verrà applicato alla regola di accesso nel campo *Inizio*, quindi passare al passaggio 4. Se si sceglie **Intervallo di indirizzi** al passaggio 1, immettere un indirizzo IP iniziale che verrà applicato alla regola di accesso nel campo *Inizio*.



Passaggio 3. Se si sceglie **Intervallo di indirizzi** al passaggio 1, immettere l'indirizzo IP finale che incapsulerà l'intervallo di indirizzi IP per la regola di accesso nel campo *Fine*.



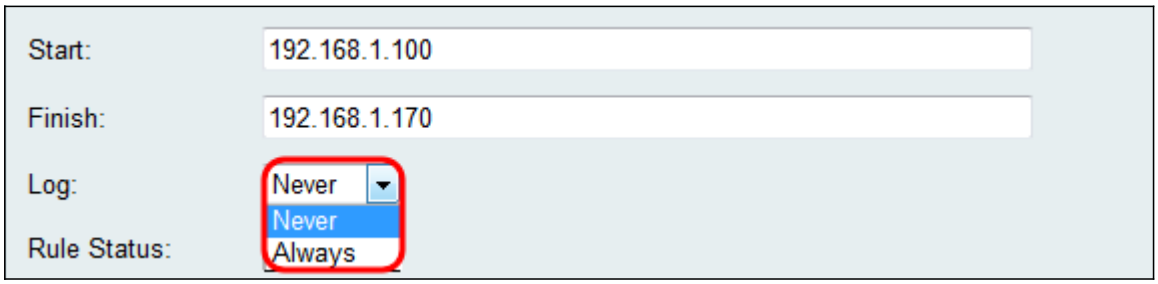
Passaggio 4. Inserire un solo indirizzo per l'IP di destinazione nel campo *Start* sotto l'elenco a discesa *IP di destinazione*. Per il traffico in entrata, l'indirizzo IP di destinazione è l'indirizzo (nella LAN) al quale il traffico proveniente dalla rete Internet pubblica è autorizzato o rifiutato.



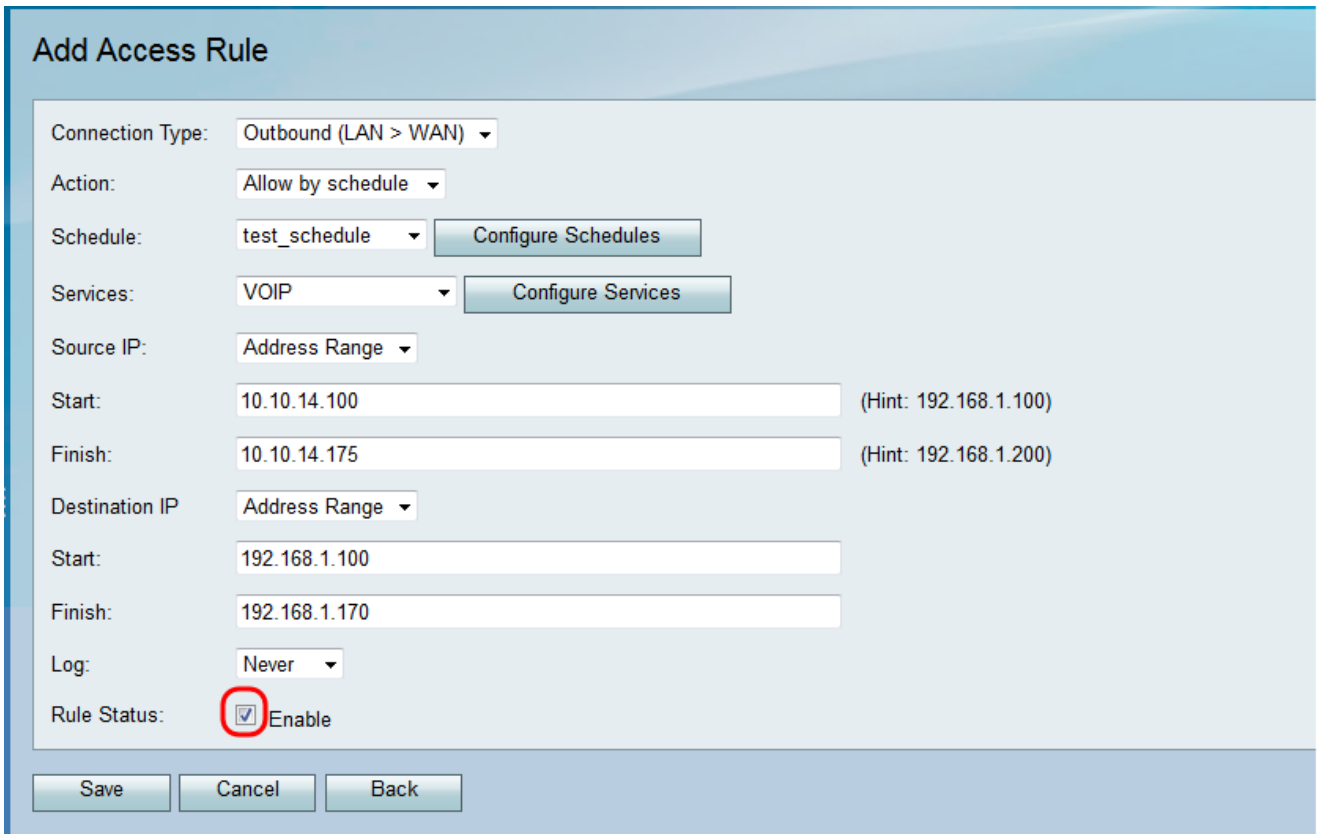
Nota: Se come Tipo di connessione è stato selezionato **In entrata (WAN > DMZ)** nel Passaggio 3 di *Aggiunta di una regola di accesso*, l'Indirizzo singolo per l'IP di destinazione viene configurato automaticamente con l'indirizzo IP dell'host DMZ abilitato.

Registrazione e attivazione della regola di accesso

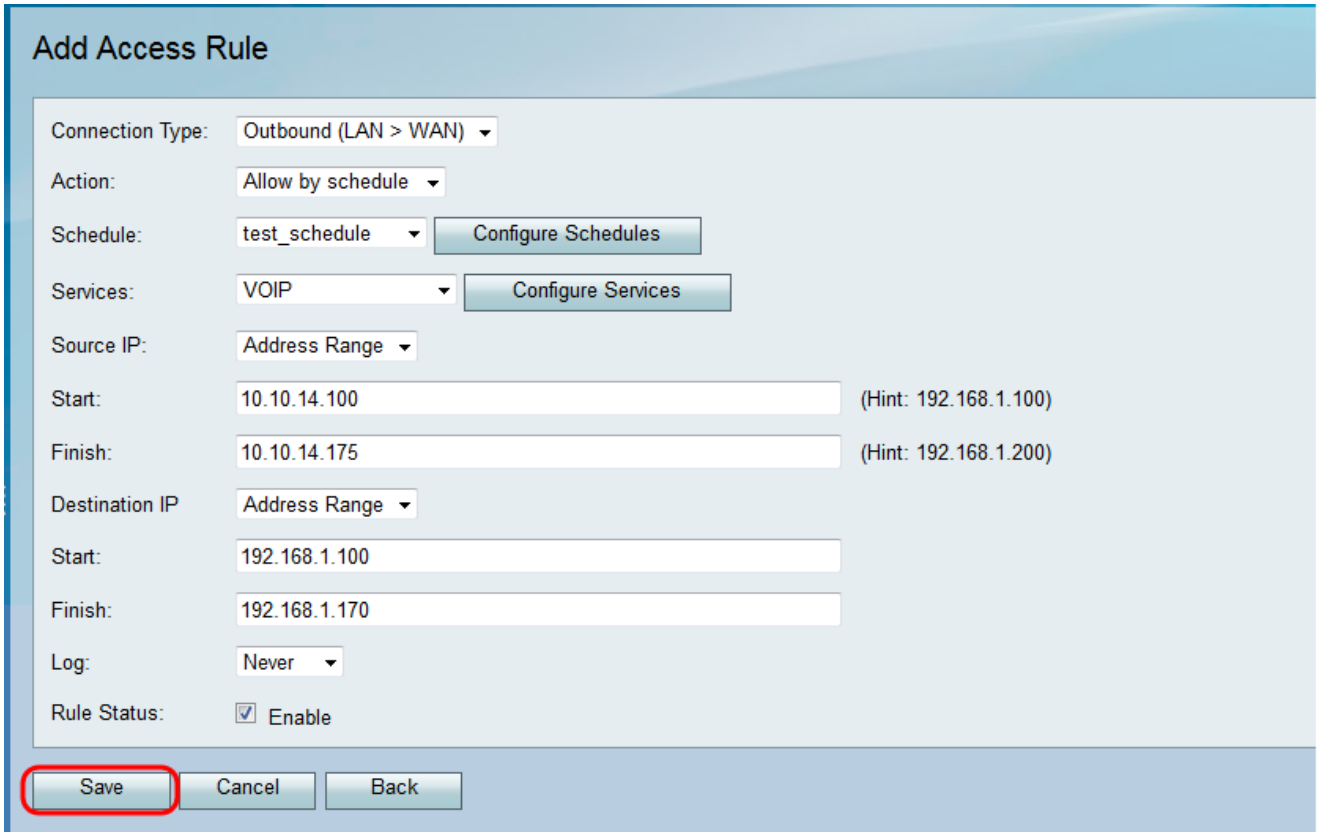
Passaggio 1. Selezionare **Sempre** nell'elenco a discesa *Log* se si desidera che il router crei i log ogni volta che un pacchetto soddisfa una regola. Selezionare **Mai** se si desidera che la registrazione non venga mai eseguita quando una regola viene soddisfatta.



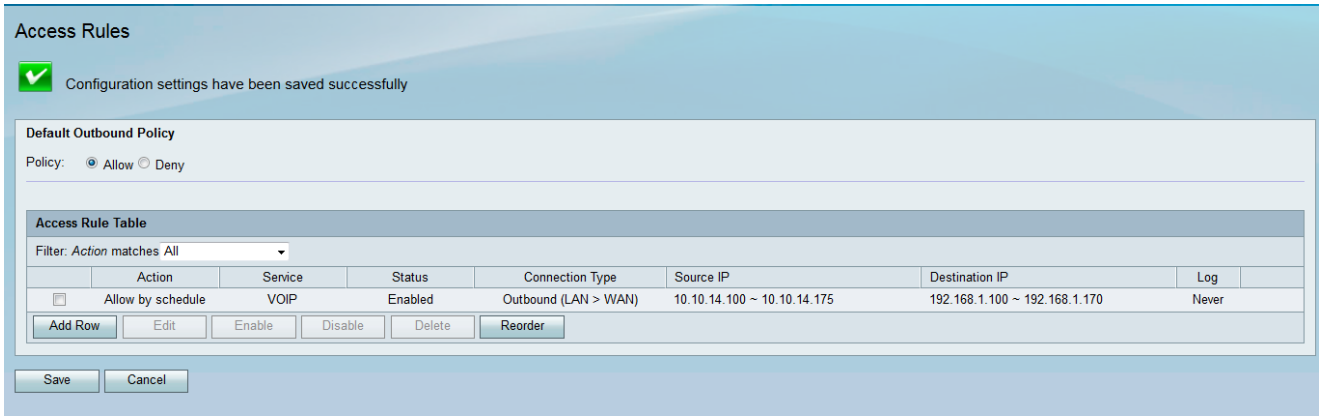
Passaggio 2. Selezionare la casella di controllo **Abilita** per abilitare la regola di accesso.



Passaggio 3. Fare clic su **Save** (Salva) per salvare le impostazioni.



La *tabella Regole di accesso* viene aggiornata con la nuova regola di accesso configurata.


Access Rules
Configuration settings have been saved successfully
Default Outbound Policy
Policy: Allow Deny
Access Rule Table
Filter: Action matches All
Action
Service
Status
Connection Type
Source IP
Destination IP
Log
Allow by schedule
VOIP
Enabled
Outbound (LAN > WAN)
10.10.14.100 ~ 10.10.14.175
192.168.1.100 ~ 192.168.1.170
Never
Add Row
Edit
Enable
Disable
Delete
Reorder
Save
Cancel

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).