Configurazione delle regole di accesso su RV215W

Obiettivo

RV215W consente di configurare le regole di accesso per aumentare la sicurezza. Questi Access Control Lists (ACLs) sono elenchi che bloccano o consentono l'invio di traffico da e verso determinati utenti. Possono essere configurati in modo da essere sempre attivi o in base a pianificazioni definite.

In questo documento viene spiegato come configurare le regole di accesso per RV215W.

Dispositivi interessati

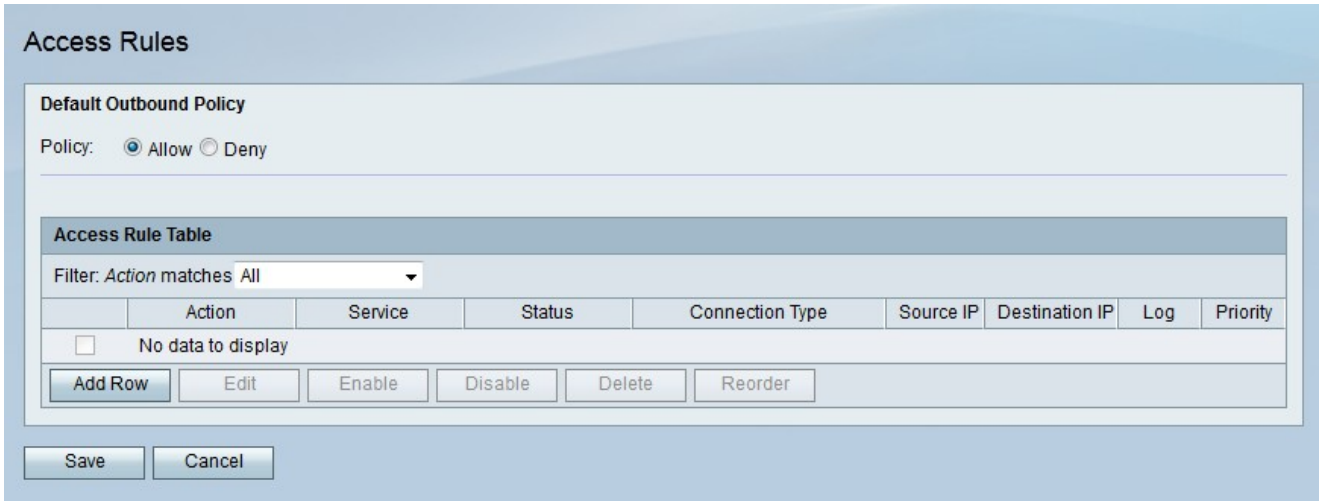
RV215W

Versione del software

•1.1.0.5

Regole di accesso

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



Passaggio 2. Fare clic sul pulsante di opzione corrispondente al criterio in uscita predefinito desiderato nel campo Criterio. Il criterio predefinito per il traffico in uscita determina se il traffico in uscita è consentito o negato. Viene utilizzato quando non esistono regole di accesso o criteri di accesso a Internet configurati per l'indirizzo IP di un utente.

Passaggio 3. Fare clic su **Salva**.

Aggiungi regola di accesso

Passaggio 1. Fare clic su **Aggiungi riga** per aggiungere una nuova regola di accesso. Viene

visualizzata la pagina Aggiungi regola di accesso:

Passaggio 2. Dall'elenco a discesa Tipo di connessione scegliere il tipo di regola da creare.

·In uscita (LAN > WAN): la regola influenza i pacchetti provenienti dalla LAN protetta e diretti alla WAN non protetta.

·In entrata (WAN > LAN): la regola influenza i pacchetti provenienti dalla WAN non protetta e diretti alla LAN protetta.

·In entrata (WAN > DMZ): la regola influenza i pacchetti provenienti dalla WAN non protetta e diretti alla DMZ. Una DMZ è un segmento di rete che separa la LAN dalla WAN per fornire un ulteriore livello di sicurezza.

Passaggio 3. Dall'elenco a discesa Azione scegliere l'azione da applicare alla regola.

·Blocca sempre: blocca sempre i pacchetti.

·Consenti sempre - Consente sempre i pacchetti.

·Blocca in base alla pianificazione: blocca i pacchetti in base a una pianificazione specificata.

·Consenti in base alla pianificazione: consente i pacchetti in base a una pianificazione specificata.

Passo 4: dall'elenco a discesa Programma scegliere un programma da applicare alla regola.

Passaggio 5. Dall'elenco a discesa Servizi scegliere un servizio da consentire o bloccare.

Nota: Fare clic su **Configura servizi** per configurare le pianificazioni nella pagina *Gestione servizi*.

Passaggio 6. Dall'elenco a discesa Source IP (IP origine), selezionare gli indirizzi IP di origine verso cui la regola blocca o consente i pacchetti.

·Qualsiasi - La regola si applica a tutti gli indirizzi IP di origine.

·Indirizzo singolo: immettere un singolo indirizzo IP a cui applicare la regola nel campo Inizio.

·Intervallo indirizzi: immettere un intervallo di indirizzi IP a cui si applica la regola nei campi Inizio e Fine.

Passaggio 7. Dall'elenco a discesa IP di destinazione scegliere gli indirizzi IP di destinazione a cui la regola blocca o consente i pacchetti.

·Qualsiasi - La regola si applica a tutti gli indirizzi IP di destinazione.

·Indirizzo singolo: immettere un singolo indirizzo IP a cui si applica la regola nel campo Inizio.

·Intervallo indirizzi: immettere un intervallo di indirizzi IP a cui si applica la regola nei campi Inizio e Fine.

Passaggio 8. Dall'elenco a discesa Registro scegliere un'opzione di registro. I registri sono record di sistema generati e utilizzati per la gestione della sicurezza.

·Mai - Disattiva i registri.

·Sempre: RV215W crea un registro ogni volta che un pacchetto soddisfa la regola.

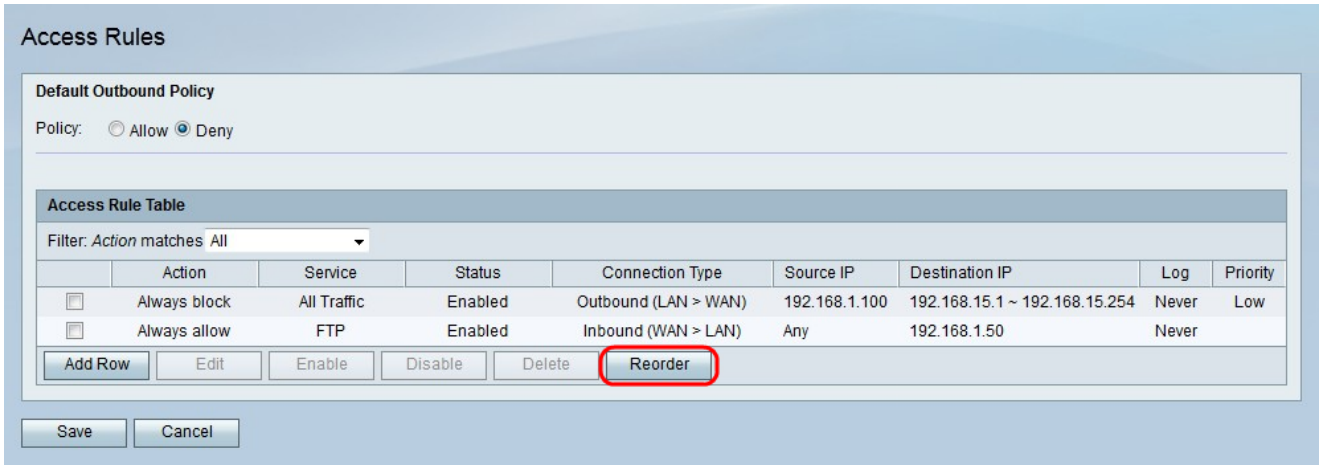
Passaggio 9. Dall'elenco a discesa Priorità QoS scegliere una priorità per i pacchetti IP in uscita della regola. La priorità uno è la più bassa, la priorità quattro è la più alta. I pacchetti nelle code con priorità più alta verranno inviati prima di quelli nelle code con priorità più bassa.

Passaggio 10. Selezionare **Abilita** nel campo Stato regola per abilitare la regola.

Passaggio 11. Fare clic su **Salva**.

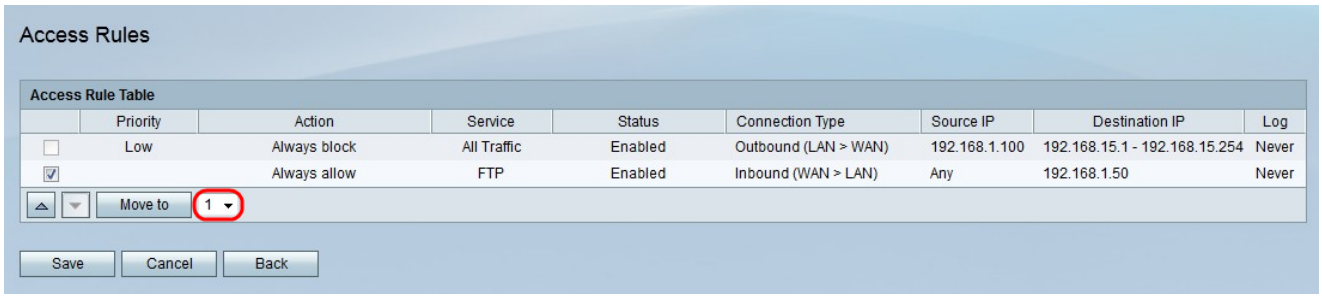
Riordina regole di accesso

La funzione di riordino è un'opzione importante del modello RV215W. L'ordine di visualizzazione delle regole di accesso nella tabella delle regole di accesso indica l'ordine di applicazione delle regole. La prima regola della tabella è la prima regola da applicare.



Passaggio 1. Fare clic su **Riordina** per riordinare le regole di accesso.

Passaggio 2. Selezionare la casella della regola di accesso che si desidera riordinare.



Passaggio 3. Dall'elenco a discesa scegliere la posizione in cui si desidera spostare la regola specificata.

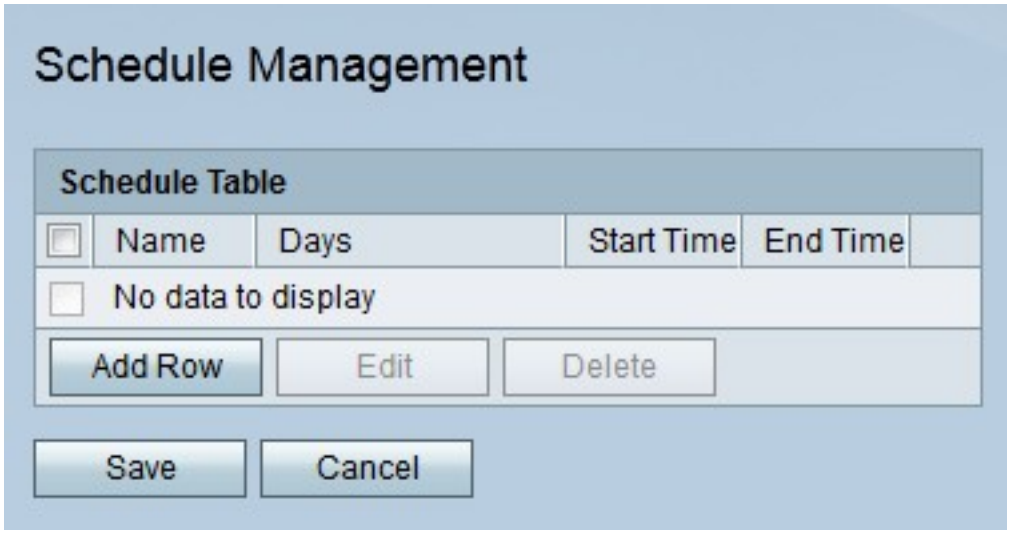
Passaggio 4. Fare clic su **Sposta in** per riordinare la regola. La regola viene spostata nella posizione specificata nella tabella.

Nota: I pulsanti freccia su e giù possono essere utilizzati anche per riordinare le regole di accesso.

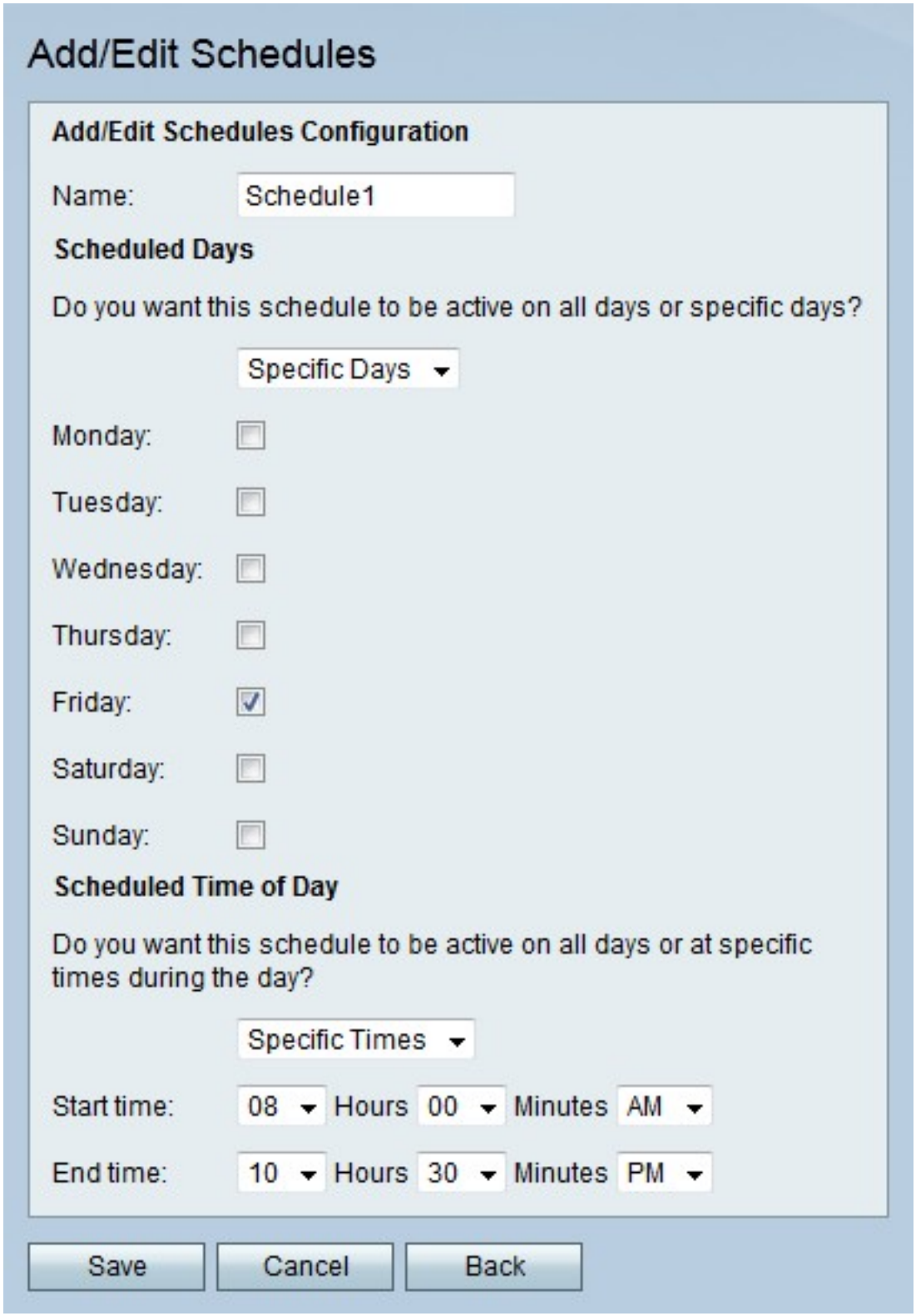
Passaggio 5. Fare clic su **Salva**.

Configurazione gestione pianificazione

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



Passaggio 2. Fare clic su **Aggiungi riga** per aggiungere una nuova pianificazione. Viene visualizzata la pagina *Aggiungi/Modifica pianificazioni*:



Passaggio 3. Inserire un nome per il programma nel campo Nome.

Passo 4: dall'elenco a discesa Giorni programmati scegliere i giorni in cui il programma è attivo.

·Tutti i giorni: la pianificazione è attiva per ogni giorno della settimana.

·Giorni specifici - Selezionare le caselle di controllo dei giorni per rendere attiva la programmazione.

Passo 5: dall'elenco a discesa Ora programmata del giorno scegliere l'ora in cui il programma è attivo.

·Tutti gli orari: la programmazione è attiva in ogni momento della giornata.

·Orari specifici: dall'elenco a discesa Ora inizio e Ora fine selezionare l'ora di inizio e l'ora di fine della programmazione.

Passaggio 6. Fare clic su **Salva**.