

Configurazione delle regole di accesso sui router serie RV160 e RV260

Obiettivo

Il router è responsabile della ricezione dei dati dalla rete esterna e rappresenta la prima linea di difesa per la sicurezza della rete locale. Abilitando le regole di accesso sul router, è possibile filtrare i pacchetti in base a parametri specifici, quali l'indirizzo IP o il numero di porta. Con la procedura descritta di seguito, questo documento intende illustrare come configurare le regole di accesso per controllare meglio i pacchetti che entrano nella rete. Questo documento evidenzierà anche alcune best practice per l'utilizzo delle regole di accesso al loro pieno potenziale per la migliore sicurezza.

Dispositivi interessati

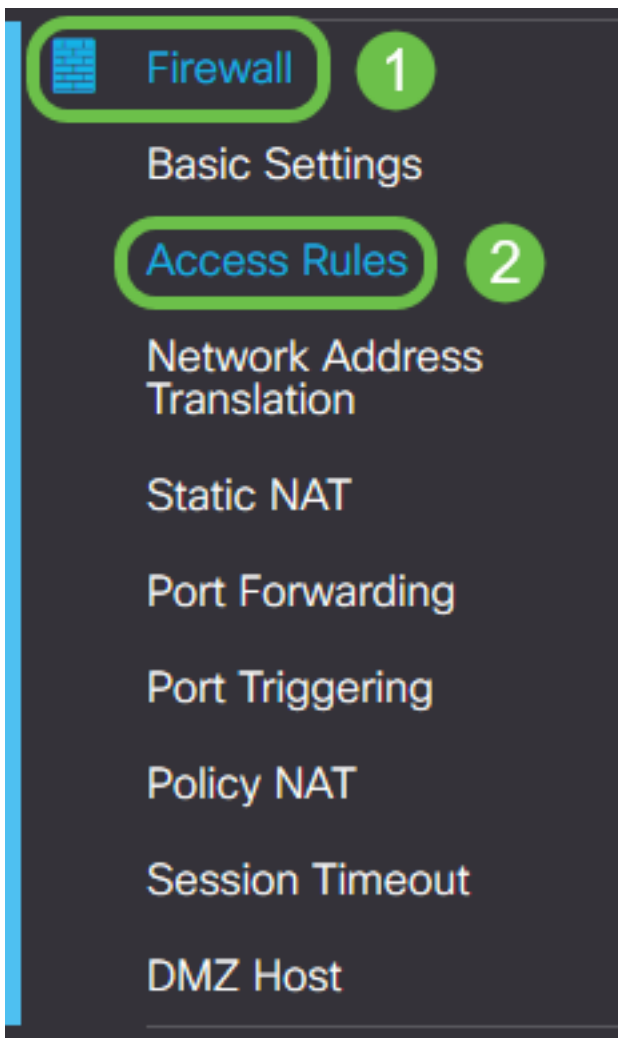
- RV160x
- RV260x

Versione del software

- 1.0.00.13

Configura regole di accesso

Passaggio 1. Dal pannello di navigazione sul lato sinistro dell'utility di configurazione, selezionare **Firewall > Regole di accesso**.



Viene visualizzata la pagina Regole di accesso. In questa pagina sono disponibili tabelle contenenti elenchi di regole di accesso e dei relativi attributi rispettivamente per IPv4 e IPv6. Da questa posizione è possibile aggiungere una nuova regola di accesso, modificare una regola esistente o rimuovere una regola esistente.

Aggiungere/modificare una regola di accesso

Passaggio 2. Per aggiungere una nuova regola di accesso, fare clic sull'icona blu da aggiungere nella tabella Regole di accesso IPv4 o Regole di accesso IPv6 a seconda del protocollo a cui si desidera applicare la regola. Nell'esempio, viene usato il protocollo IPv4.

IPv4 Access Rules Table



Per modificare una voce esistente, selezionare la casella di controllo accanto alla regola di accesso che si desidera modificare. Selezionate quindi l'icona di modifica blu nella parte superiore della tabella corrispondente. È possibile selezionare una sola regola alla volta per la modifica.

IPv4 Access Rules Table

<input checked="" type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	Any	Any	Any
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN

Viene visualizzata la pagina *Aggiungi/Modifica regole di accesso*.

Passaggio 3. Selezionare/deselezionare la casella di controllo Stato regola per abilitare o disabilitare la regola di accesso durante l'operazione. Ciò è utile quando si dispone di una regola di accesso che si desidera salvare per applicarla in un secondo momento.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Passaggio 4. Dal campo *Azione*, selezionare se la regola deve consentire o negare l'accesso al traffico di rete in ingresso da specificare.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Nota: Per una sicurezza ottimale, è consigliabile impostare regole di accesso che consentano solo il traffico che si prevede di ricevere, anziché tentare solo di negare il traffico indesiderato. Ciò consente di proteggere meglio la rete da minacce sconosciute.

Passaggio 5. Nel campo *Services* (Servizi), selezionare dal menu a discesa il tipo di servizio di rete a cui si desidera applicare la regola di accesso.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Nota: Il pulsante di opzione IPv4 o IPv6 viene selezionato automaticamente in base alla tabella a cui si è scelto di applicare la regola di accesso dalla pagina *Regole di accesso*.

Passaggio 6. Selezionare dal campo *Log* se si desidera che il router generi un messaggio di log quando i pacchetti che entrano nella rete corrispondono alle regole applicate.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Passaggio 7. Dall'elenco a discesa *Interfaccia di origine*, selezionare l'interfaccia di rete per i pacchetti in ingresso a cui verrà applicata la regola di accesso.

Log: Always Never

Source Interface: Any

Source Address: WAN
USB
VLAN1
Any

Destination Interface: Any

Destination Address: Any

Passaggio 8. Selezionare dall'elenco a discesa *Source Address* il tipo di indirizzo in ingresso a cui verrà applicata la regola di accesso. Le opzioni sono le seguenti:

- Qualsiasi: la regola verrà applicata a tutti gli indirizzi IP in ingresso.
- Singola: la regola verrà applicata a un singolo indirizzo IP definito.
- Subnet - La regola verrà applicata a una subnet definita di una rete
- Intervallo IP - La regola verrà applicata a un intervallo definito di indirizzi IP

Nota: Se si seleziona Singola, Subnet o Intervallo IP, verranno visualizzati i campi corrispondenti a destra del menu a discesa in cui è possibile immettere i dettagli dell'indirizzo. Nell'esempio, viene immesso un intervallo IP per la dimostrazione.

Source Interface: Any

Source Address: IP Range 1.2.3.1 To 1.2.3.100 (1.2.3.1 To 1.2.3.4)

Destination Interface: Any
Single
Subnet
IP Range

Destination Address:

Passaggio 9. Dall'elenco a discesa *Interfaccia di destinazione*, selezionare l'interfaccia di rete per i

pacchetti in uscita a cui verrà applicata la regola di accesso.

Log: Always Never

Source Interface: Any

Source Address: Any

Destination Interface: Any

Destination Address:

Schedule

Passaggio 10. Selezionare dall'elenco a discesa *Indirizzo di destinazione* il tipo di indirizzo in uscita a cui verrà applicata la regola di accesso. Le opzioni sono le seguenti:

- Qualsiasi: la regola verrà applicata a tutti gli indirizzi IP in uscita.
- Singola: la regola verrà applicata a un singolo indirizzo IP definito.
- Subnet - La regola verrà applicata a una subnet definita di una rete
- Intervallo IP - La regola verrà applicata a un intervallo definito di indirizzi IP

Nota: Se si seleziona Singola, Subnet o Intervallo IP, verranno visualizzati i campi corrispondenti a destra del menu a discesa in cui è possibile immettere i dettagli dell'indirizzo. In questo esempio viene immessa una subnet da dimostrare.

Destination Interface: Any

Destination Address: Subnet 1.2.3.4 / 16 (1.2.3.4 / 32)

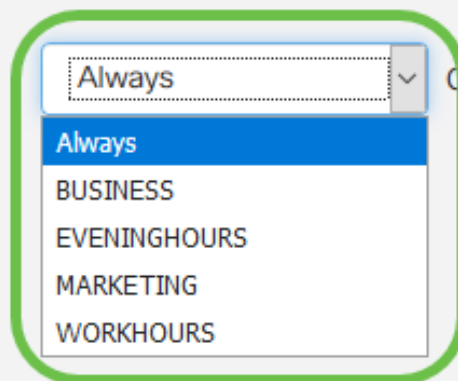
Schedule

Schedule Name: Always Click [here](#) to configure the schedules.

Passaggio 11. Dall'elenco a discesa *Nome programma* selezionare il programma temporale a cui si desidera applicare la regola di accesso.

Schedule

Schedule Name:

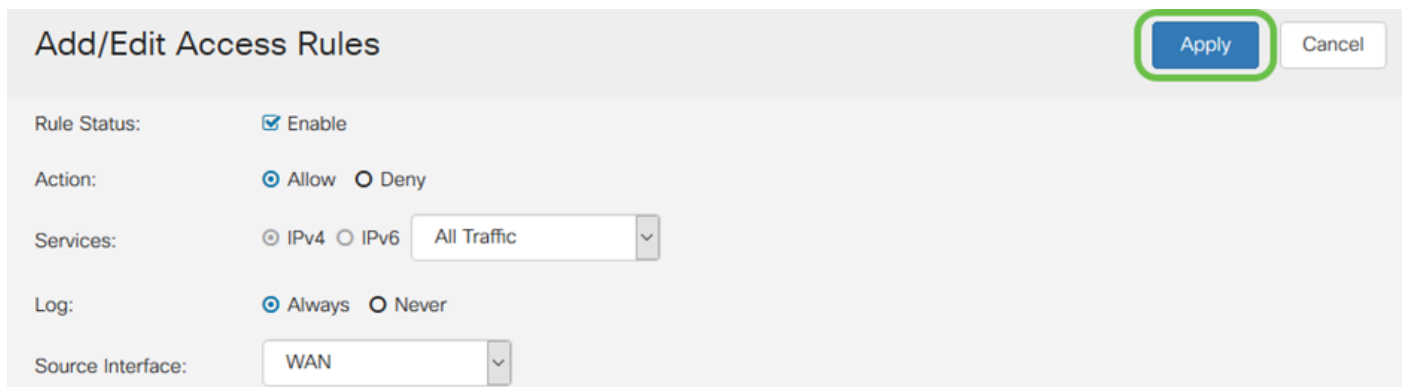


Click [here](#) to configure the schedules.

Nota: Per una maggiore sicurezza, è consigliabile limitare l'accesso non critico alla rete agli orari di lavoro, in modo da impedire connessioni indesiderate quando l'azienda non è operativa.

Nota: Fare clic sul collegamento a destra dell'elenco a discesa *Nome pianificazione* per configurare gli orari di pianificazione per le regole di accesso. Per ulteriori informazioni su come configurare queste pianificazioni, fare clic [qui](#).

Passaggio 12. Una volta completata la configurazione della regola di accesso, fare clic su **Applica** per confermare.



Add/Edit Access Rules [Apply](#) [Cancel](#)

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

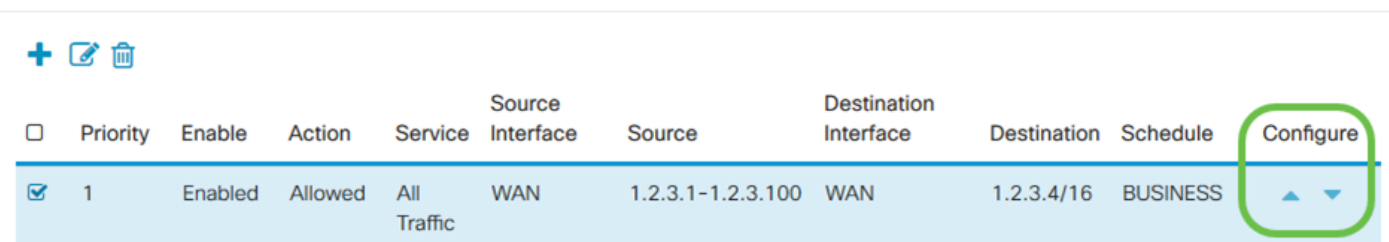
Log: Always Never


Source Interface: WAN

Verrà visualizzata di nuovo la pagina *Regole di accesso* principale.

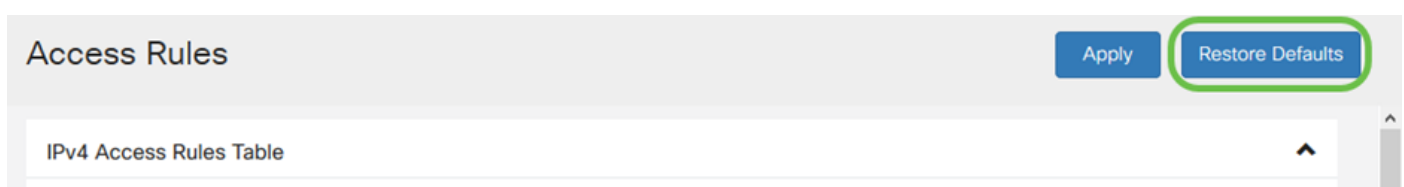
Nota: Quando viene creata una nuova regola di accesso, la relativa priorità viene posizionata in fondo all'elenco. Ciò significa che se una regola di accesso è in conflitto con un'altra regola di un parametro specifico, le restrizioni della regola con priorità più alta avranno la precedenza. Per spostare una regola verso l'alto o verso il basso in ordine di priorità, è possibile utilizzare le frecce blu nella colonna Configura.

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	

Passaggio 13 (facoltativo). Per ripristinare l'elenco delle regole di accesso ai valori predefiniti, fare clic su **Ripristina valori predefiniti** nell'angolo superiore destro della pagina.



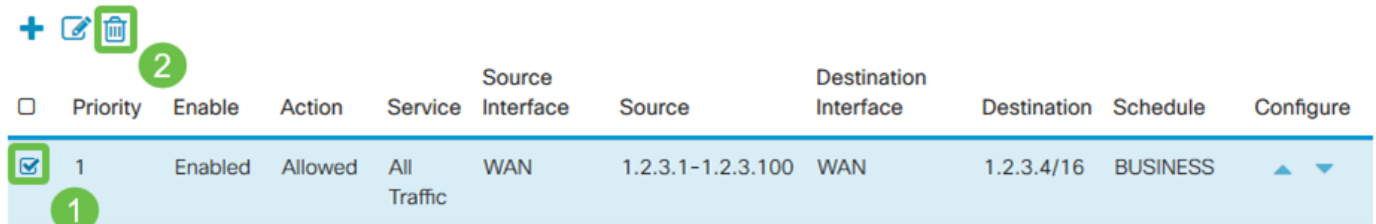
Access Rules [Apply](#) [Restore Defaults](#)

IPv4 Access Rules Table

Rimuovere una regola di accesso

Passaggio 14. Per rimuovere una regola di accesso dall'elenco, selezionare la casella di controllo corrispondente alla regola che si desidera rimuovere. Selezionare quindi l'icona blu del cestino nella parte superiore dell'elenco. È possibile rimuovere contemporaneamente più voci della regola di accesso.

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	▲ ▼

Gestione dei servizi

La gestione dei servizi consente di aggiungere o modificare i servizi di rete esistenti in base al numero di porta, al protocollo e ad altri dettagli. Questi servizi di rete saranno disponibili nell'elenco a discesa Servizi durante la configurazione delle regole di accesso. Tramite il menu di configurazione dell'elenco di gestione dei servizi è possibile creare servizi personalizzati che possono essere applicati alle regole di accesso per un controllo più accurato del traffico in entrata nella rete. Per ulteriori informazioni su come configurare Gestione servizi, fare clic [qui](#).

Conclusioni

Le regole di accesso, se applicate in modo appropriato, sono uno strumento prezioso per proteggere la connessione WAN. Con la guida e le procedure descritte sopra, è possibile disporre di tutto il necessario per configurare correttamente regole di accesso sicuro per il router RV160x o RV260x.