

Configurazione delle regole di accesso su un router serie RV34x

Obiettivo

RV340 Dual-WAN VPN Router è un dispositivo flessibile, ad alte prestazioni e facile da usare, ideale per le piccole aziende. Con funzionalità di protezione aggiuntive, ad esempio Filtro Web, Controllo applicazione e Protezione origine IP. Il nuovo RV340 offre connettività cablata a banda larga e ad alta sicurezza per piccoli uffici e dipendenti remoti. Queste nuove funzioni di sicurezza consentono inoltre di regolare con facilità le attività consentite sulla rete.

Le regole o i criteri di accesso sul router serie RV34x consentono di configurare le regole per aumentare la sicurezza della rete. Una combinazione di regole e si dispone di un Access Control List (ACL). Gli ACL sono elenchi che bloccano o consentono l'invio di traffico da e verso determinati utenti. È possibile configurare le regole di accesso in modo che siano sempre attive o basate su pianificazioni definite.

Alla fine dell'elenco, gli ACL hanno un rifiuto implicito, quindi il traffico non può passare a meno che non lo si autorizzi esplicitamente. Ad esempio, se si desidera consentire a tutti gli utenti di accedere a una rete tramite il router, ad eccezione di determinati indirizzi, è necessario negare gli indirizzi particolari e quindi consentire tutti gli altri.

In questo articolo viene spiegato come configurare le regole di accesso su un router serie RV34x.

Dispositivi interessati

- Serie RV34x

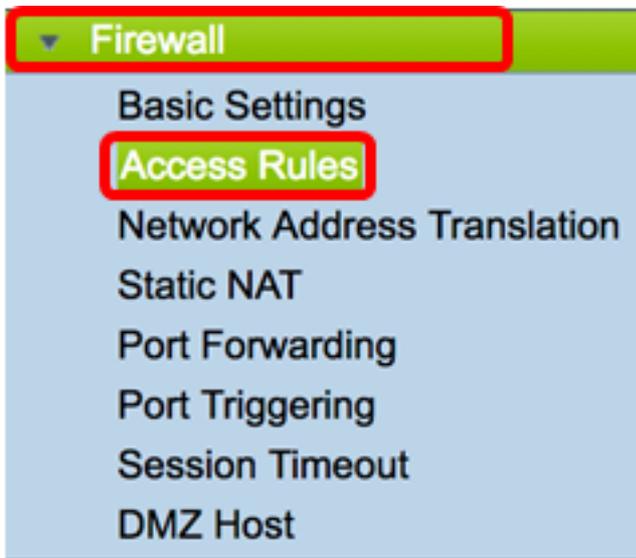
Versione del software

- 1.0.1.16
 - [Dopo la pubblicazione di questo articolo è disponibile un aggiornamento del firmware dell'interfaccia utente. Fare clic qui per andare alla pagina dei download e individuare il prodotto specifico.](#)

Configurazione di una regola di accesso su un router serie RV34x

Creare una regola di accesso

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Firewall > Regole di accesso**.



Passaggio 2. Nella tabella Regole di accesso IPv4 o IPv6 fare clic su **Aggiungi** per creare una nuova regola.

Nota: Sui router serie RV34x è possibile configurare fino a 202 regole. Nell'esempio viene usato il protocollo IPv4.

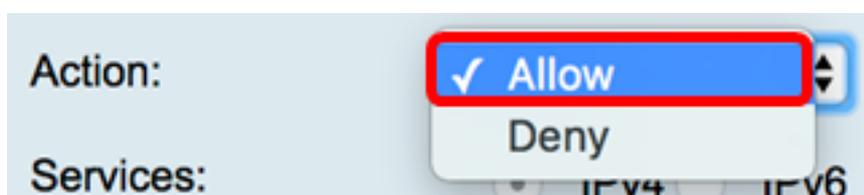


Passaggio 3. Selezionare la casella di controllo **Abilita stato regola** per abilitare la regola.



Passaggio 4. Nel menu a discesa Azione, scegliere se il criterio consentirà o negherà i dati.

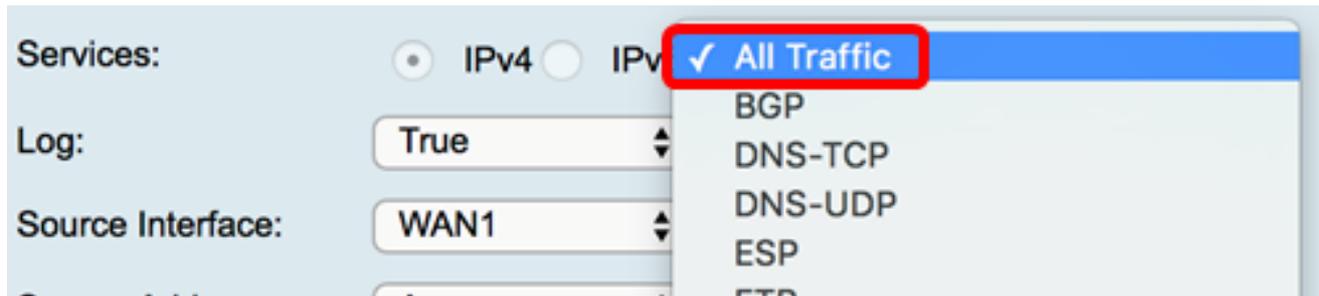
Nota: Nell'esempio riportato di seguito viene scelto Consenti.



Passaggio 5. Dal menu a discesa Servizi, scegliere il tipo di traffico che il router consentirà o

negherà.

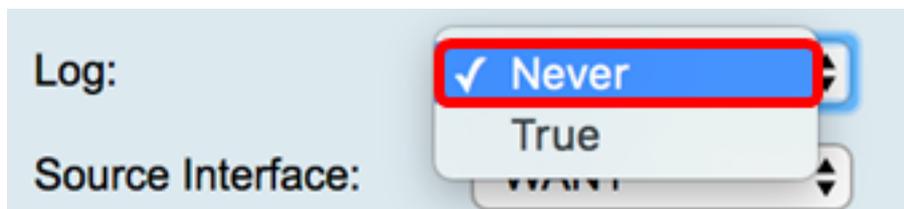
Nota: Per questo esempio, viene scelto Tutto il traffico. Tutto il traffico sarà autorizzato.



Passaggio 6. Dal menu a discesa Log, scegliere un'opzione per determinare se il router registrerà il traffico autorizzato o rifiutato. Le opzioni sono:

- Mai: il router non registrerà mai il traffico autorizzato e rifiutato.
- True: il router registrerà il traffico che corrisponde al criterio.

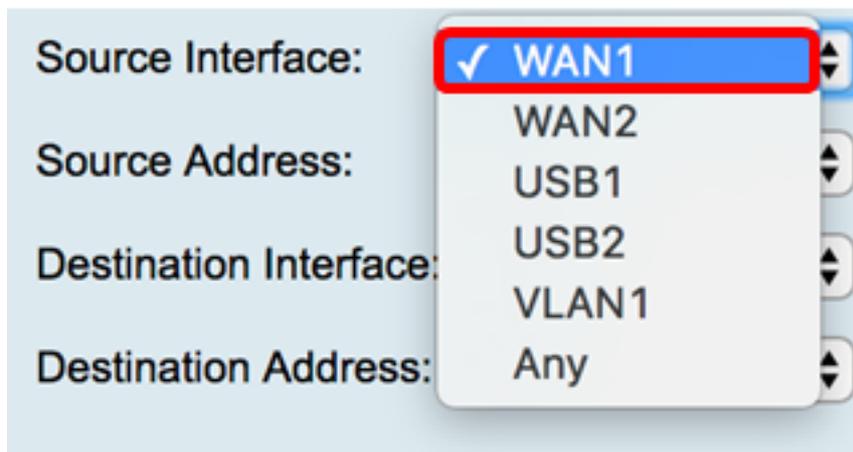
Nota: Nell'esempio viene scelto Mai.



Passaggio 7. Dal menu a discesa Interfaccia di origine, scegliere un'interfaccia per il traffico in entrata o in entrata a cui applicare i criteri di accesso. Le opzioni sono

- WAN1: il criterio si applica solo al traffico proveniente da WAN1.
- WAN2 - Il criterio si applica solo al traffico proveniente da WAN2.
- USB1: il criterio si applica solo al traffico proveniente da USB1.
- USB2 — il criterio si applica solo al traffico proveniente da USB2.
- VLAN1: il criterio si applica solo al traffico VLAN1.
- Any: il criterio si applica a qualsiasi interfaccia.

Nota: Se è stata configurata una VLAN (Virtual Local Area Network) aggiuntiva, l'opzione VLAN viene visualizzata nell'elenco. Nell'esempio, viene scelta WAN1.

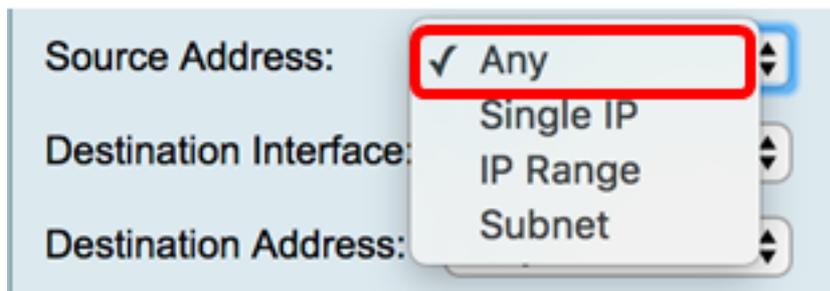


Passaggio 8. Dal menu a discesa Indirizzo di origine, scegliere un'origine per applicare il

criterio. Le opzioni sono:

- Qualsiasi - Il criterio verrà applicato a qualsiasi indirizzo IP della rete. Se si sceglie questa opzione, andare al [passaggio 12](#).
- IP singolo: il criterio si applica a un singolo host o indirizzo IP. Se si sceglie questa opzione, andare al [passaggio 9](#).
- Intervallo IP: il criterio si applica a un set o a un intervallo di indirizzi IP. Se si sceglie questa opzione, andare al [passaggio 10](#).
- Subnet: il criterio si applica a un'intera sottorete. Se si sceglie questa opzione, andare al [passaggio 11](#).

Nota: Nell'esempio, viene scelto Qualsiasi.



The image shows a configuration panel with three fields: 'Source Address', 'Destination Interface', and 'Destination Address'. A dropdown menu is open for 'Source Address', showing four options: 'Any' (with a checkmark), 'Single IP', 'IP Range', and 'Subnet'. The 'Any' option is highlighted with a red box.

[Passaggio 9](#). (Facoltativo) Nel passaggio 8 è stato scelto un solo indirizzo IP, immettere un solo indirizzo IP per il criterio da applicare, quindi andare al [passaggio 12](#).

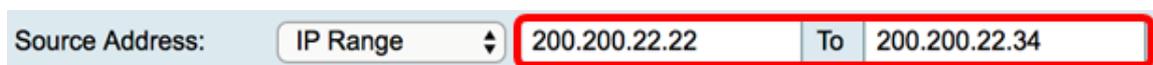
Nota: Nell'esempio, viene usato 200.200.22.52.



The image shows a configuration panel for 'Source Address'. The dropdown menu is set to 'Single IP'. The text input field contains the IP address '200.200.22.52', which is highlighted with a red box.

[Passaggio 10](#). (Facoltativo) Se nel passaggio 8 è stato scelto Intervallo IP, immettere gli indirizzi IP iniziale e finale nei campi dell'indirizzo IP corrispondenti.

Nota: Nell'esempio, 200.200.22.22 viene usato come indirizzo IP iniziale e 200.200.22.34 come indirizzo IP finale.



The image shows a configuration panel for 'Source Address'. The dropdown menu is set to 'IP Range'. There are two text input fields: the first contains '200.200.22.22' and the second contains '200.200.22.34'. Both fields are highlighted with a red box.

[Passaggio 11](#). (Facoltativo) Se nel passaggio 8 è stata scelta una subnet, immettere l'ID di rete e la subnet mask corrispondente per applicare il criterio.

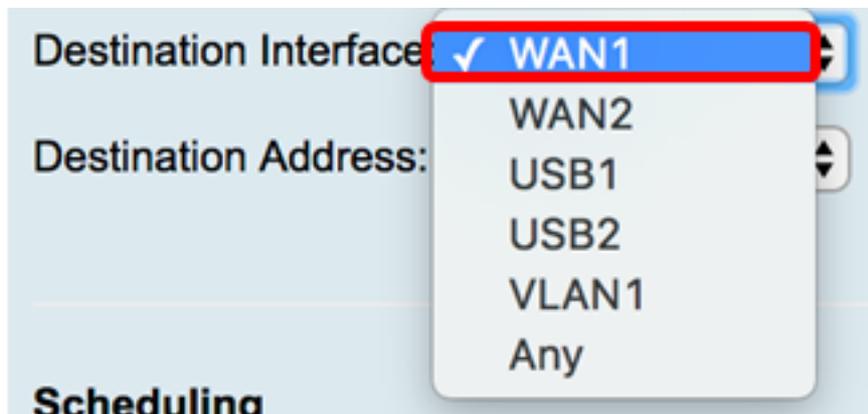
Nota: Nell'esempio, 200.200.22.1 viene usato come ID subnet e 24 come subnet mask.



The image shows a configuration panel for 'Source Address'. The dropdown menu is set to 'Subnet'. There are two text input fields: the first contains '200.200.22.1' and the second contains '24'. Both fields are highlighted with a red box.

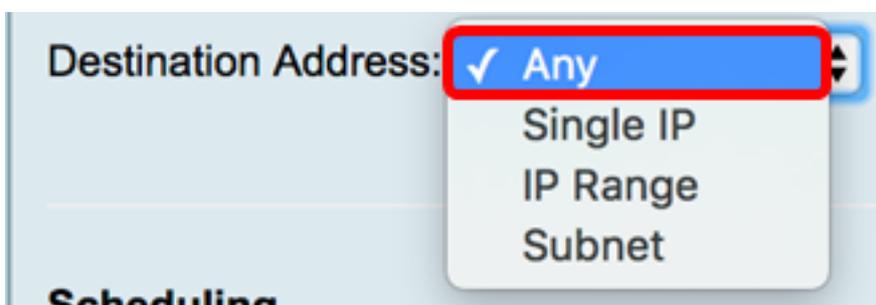
[Passaggio 12](#). Dal menu a discesa Interfaccia di destinazione, scegliere un'interfaccia per il traffico in uscita o in uscita a cui applicare i criteri di accesso. Le opzioni sono WAN1, WAN2, USB1, USB2, VLAN1 e Any.

Nota: Per questo esempio, viene scelta WAN1.



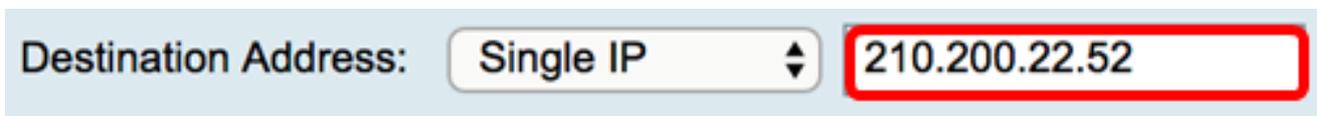
Passaggio 13. Dal menu a discesa Indirizzo di destinazione, scegliere una destinazione a cui applicare il criterio. Le opzioni sono Any, Single IP, IP Range, Subnet.

Nota: Nell'esempio, viene scelto Qualsiasi. Andare al [passo 17](#).



Passaggio 14. (Facoltativo) Se nel passaggio 13 è stato scelto IP singolo, immettere un indirizzo IP singolo per il criterio da applicare.

Nota: Nell'esempio, viene usato 210.200.22.52.



Passaggio 15. (Facoltativo) Se nel Passaggio 13 è stato scelto Intervallo IP, immettere gli indirizzi IP iniziale e finale nei rispettivi campi di indirizzi IP.

Nota: Nell'esempio, l'indirizzo IP iniziale è 210.200.27.22 e l'indirizzo IP finale è 210.200.27.34. Andare al [passo 17](#).

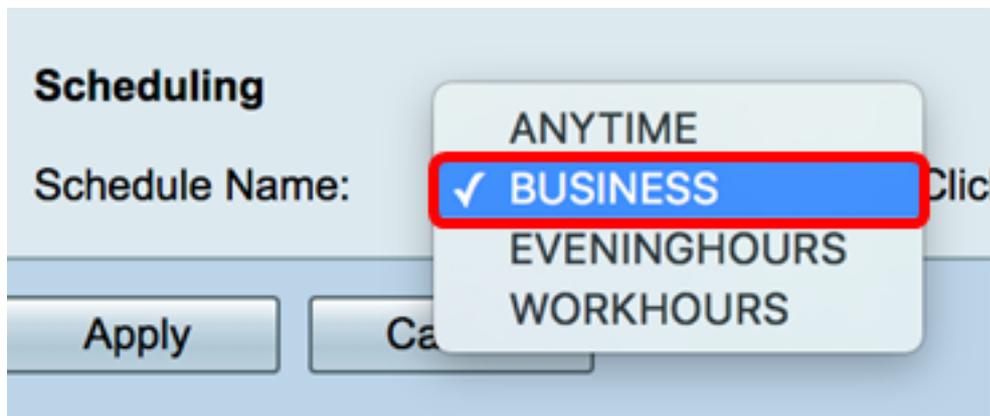


Passaggio 16. (Facoltativo) Se nel passaggio 13 è stata scelta una subnet, immettere l'indirizzo di rete e la subnet mask corrispondente per applicare il criterio.

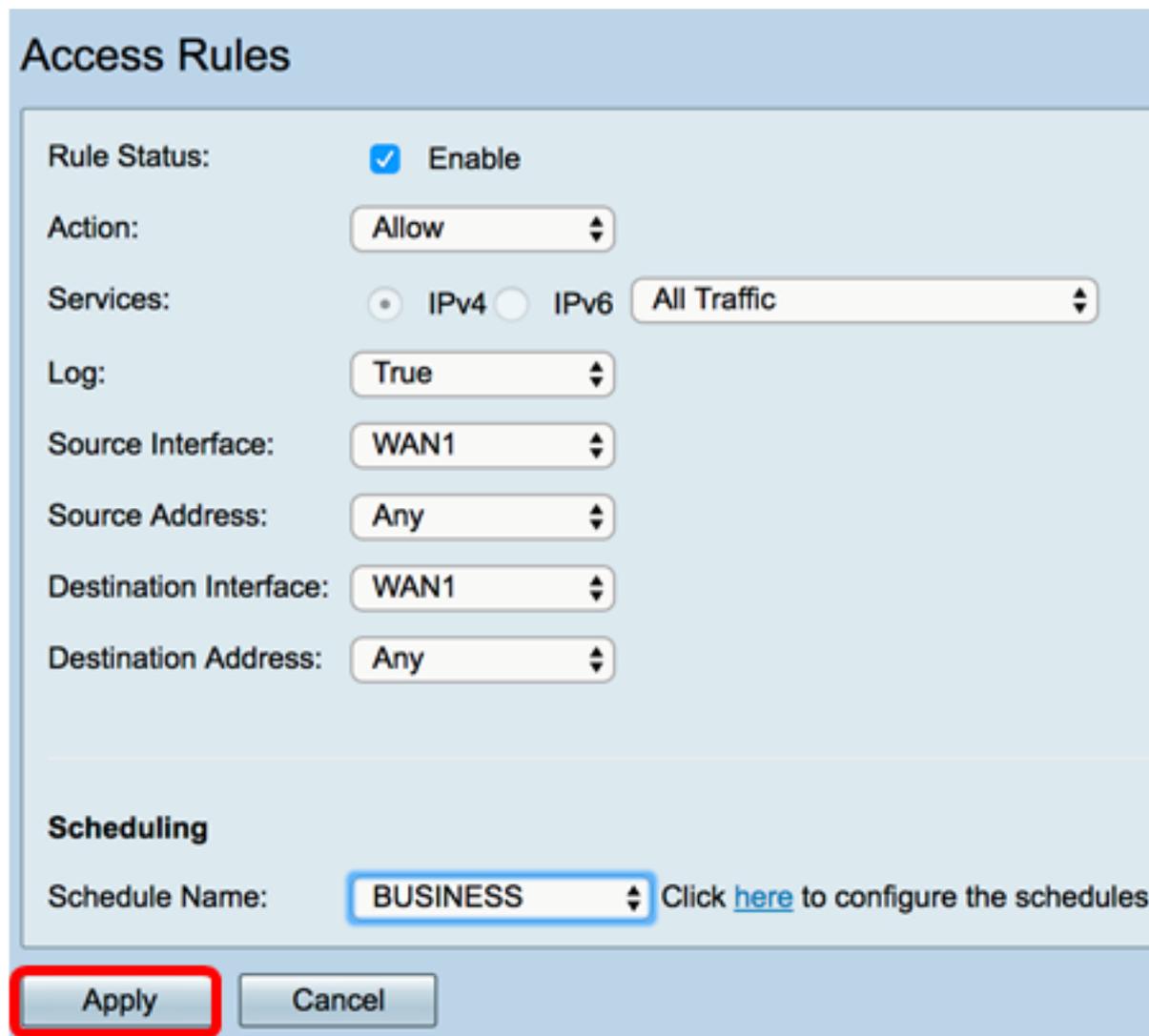
Nota: Nell'esempio, 210.200.27.1 viene usato come indirizzo di subnet e 24 come subnet mask.



[Passaggio 17](#). Dall'elenco a discesa Nome programmazione scegliere una programmazione a cui applicare il criterio. per informazioni su come configurare una pianificazione, fare clic [qui](#).



Passaggio 18. Fare clic su **Applica**.



A questo punto, è necessario creare una regola di accesso su un router serie RV.

Modificare una regola di accesso

Passaggio 1. Nella tabella Regole di accesso IPv4 o IPv6 selezionare la casella di controllo accanto alla regola di accesso che si desidera configurare.

Nota: Nell'esempio, nella tabella Regole di accesso IPv4, viene scelta la priorità 1.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Passaggio 2. Fare clic su **Modifica**.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Passaggio 3. (Facoltativo) Nella colonna Configura fare clic sul pulsante **Modifica** nella riga della regola di accesso desiderata.

Schedule	Configure			
BUSINESS	<input checked="" type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
BUSINESS	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

Passaggio 4. Aggiornare i parametri necessari.

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

Apply

Cancel

Passaggio 5. Fare clic su **Applica**.

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

Passaggio 6. (Facoltativo) Per modificare la priorità di una regola di accesso nella colonna Configura, fare clic sul pulsante **Su** o **Giù** della regola di accesso che si desidera spostare.

Nota: Quando una regola di accesso viene spostata verso l'alto o verso il basso, si sposta di un passo al di sopra o al di sotto della posizione originale. In questo esempio, la priorità 1 verrà spostata verso il basso.

Priority	Enable	Action	Service	Source Interf...	Source	Destinat...	Destination	Schedule	Configure
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	WAN1	Any	USB1	192.168.1.1	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 201	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	VLAN	Any	WAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 202	<input checked="" type="checkbox"/>	Denied	IPv4: All T...	WAN	Any	VLAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>

Nota: Nell'esempio, la priorità 1 è ora la priorità 2.

IPv4 Access Rules Table										
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter...	Source	Destina...	Destination	Schedule	Configure
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	VLAN	Any	WAN	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Tr...	WAN	Any	VLAN	Any	ANYTIME	Edit Delete Up Down

Add Edit Delete

Passaggio 7. Fare clic su **Applica**.

Access Rules

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Add Edit Delete

IPv6 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

Add Edit Delete

Apply
Restore to Default Rules
Service Management

A questo punto, è possibile modificare una regola di accesso su un router serie RV34x.

Eliminare una regola di accesso

Passaggio 1. Nella tabella Regole di accesso IPv4 o IPv6 selezionare la casella di controllo accanto alla regola di accesso che si desidera eliminare.

Nota: Nell'esempio, nella tabella Regole di accesso IPv4, viene scelta la priorità 1.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Passaggio 2. Fare clic su **Delete** situato sotto la tabella o sul pulsante Delete nella colonna Configure.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Passaggio 3. Fare clic su **Applica**.

Access Rules

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

IPv6 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

A questo punto, è necessario eliminare una regola di accesso sul router serie RV34x.

[Qui è disponibile un video relativo a questo articolo...](#)

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)