

Configurazione delle regole di accesso sui router VPN RV320 e RV325

Obiettivo

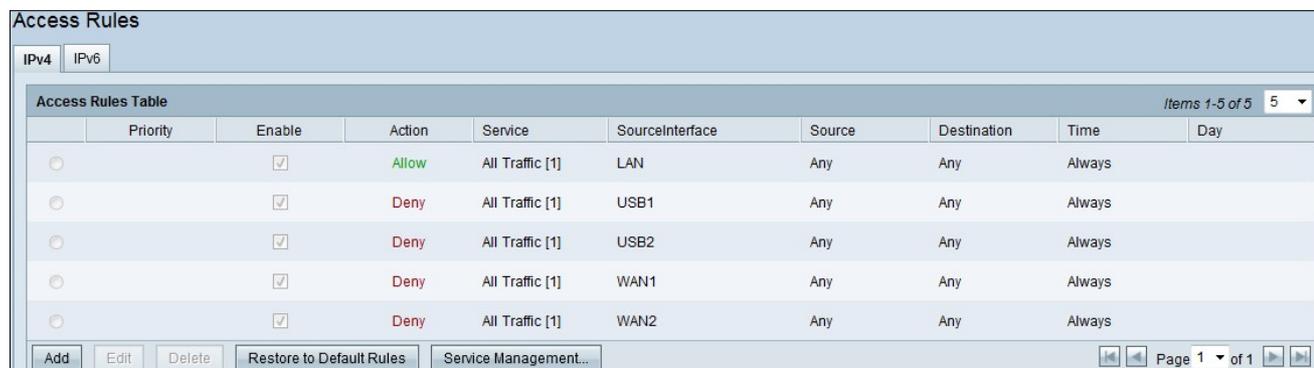
Gli Access Control Lists (ACLs) sono elenchi che bloccano o consentono l'invio di traffico da e verso determinati utenti. È possibile configurare le regole di accesso in modo che siano sempre attive o basate su una pianificazione definita. Una regola di accesso viene configurata in base a diversi criteri per consentire o negare l'accesso alla rete. La regola di accesso viene pianificata in base all'ora in cui le regole di accesso devono essere applicate al router. In questo articolo viene descritta la Configurazione guidata regole di accesso utilizzata per determinare se il traffico può entrare nella rete attraverso il firewall del router o meno per garantire la sicurezza della rete.

Dispositivi interessati | Versione firmware

- RV320 Dual WAN VPN Router | V 1.1.0.09 ([scarica la versione più recente](#))
- RV325 Gigabit Dual WAN VPN Router | V 1.1.0.09 ([scarica la versione più recente](#))

Configurazione regola di accesso

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



Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

La tabella Regole di accesso contiene le informazioni riportate di seguito.

- **Priorità:** visualizza la priorità della regola di accesso
- **Abilita** - mostra se la regola di accesso è abilitata o disabilitata
- **Azione:** visualizza la regola di accesso consentita o negata.
- **Servizio:** visualizza il tipo di servizio.
- **SourceInterface:** visualizza l'interfaccia a cui viene applicata la regola di accesso.
- **Source** - Visualizza l'indirizzo IP del dispositivo di origine
- **Destinazione:** visualizza l'indirizzo IP del dispositivo di destinazione.
- **Ora:** visualizza l'ora in cui la regola di accesso deve essere applicata
- **Giorno:** viene visualizzato durante una settimana in cui viene applicata la regola di accesso

Gestione dei servizi

Passaggio 1. Fare clic su **Gestione servizi** per aggiungere un nuovo servizio. Viene visualizzata la

tabella Gestione assistenza:

The screenshot shows a web interface titled "Service Management Table". At the top right, it indicates "Items 1-5 of 21" and "5 per page". The table has four columns: "Service Name", "Protocol", and "Port Range". There are five rows of data, each with a checkbox in the first column. Below the table are buttons for "Add", "Edit", and "Delete", along with pagination controls showing "Page 1 of 5". At the bottom of the interface are "Save" and "Cancel" buttons.

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080

Passaggio 2. Fare clic su **Add** per aggiungere un nuovo servizio.

This screenshot is similar to the previous one, but the "Add" button is highlighted with a red circle. Below the table, a new row is being added with the following values: "Database" in the Service Name field, "TCP" in the Protocol dropdown, and "520 ~ 520" in the Port Range field. The "Add" button is also highlighted with a red circle.

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080
<input type="checkbox"/>	Database	TCP	520 ~ 520

Passaggio 3. Configurare i campi seguenti.

- Nome servizio: in base ai requisiti, fornire un nome per il servizio
- Protocollo: scegliere un protocollo TCP o UDP per il servizio
- Intervallo porte: immettere l'intervallo di numeri di porta in base alle proprie esigenze e il numero di porta deve essere compreso nell'intervallo (1-65536).

Passaggio 4. Fare clic su **Salva** per salvare le modifiche

Configurazione delle regole di accesso su IPv4

Access Rules									
Access Rules Table Items 1-5 of 5 5 per page									
Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day	
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Page 1 of 1

Passaggio 1. Fare clic su **Add** per configurare una nuova regola di accesso. Viene visualizzata la finestra *Modifica regole di accesso*.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 2. Scegliere l'opzione appropriata dall'elenco a discesa Azione per consentire o limitare il traffico per la regola che si sta impostando. Le regole di accesso limitano l'accesso alla rete in base a vari valori.

- Consenti — consente tutto il traffico.
- Nega — limita tutto il traffico.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on: Mon Tue Wed Thu Fri Sat

Passaggio 3. Scegliere il servizio appropriato da filtrare dall'elenco a discesa Servizio.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 4. Scegliere l'opzione Log appropriata dall'elenco a discesa Log. L'opzione log determina se il dispositivo mantiene un registro del traffico che corrisponde alle regole di accesso impostate.

- Registra pacchetti corrispondenti a questa regola di accesso: il router conserva un registro che tiene traccia del servizio selezionato.
- Not Log: il router non conserva i log per la regola di accesso.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Passo 5: dall'elenco a discesa Interfaccia, scegliere l'interfaccia di origine appropriata. In questa interfaccia viene applicata la regola di accesso.

- LAN: la regola di accesso influisce solo sul traffico LAN.
- WAN 1: la regola di accesso influenza solo il traffico WAN 1.
- WAN 2: la regola di accesso influenza solo il traffico WAN 2.
- Qualsiasi - La regola di accesso influisce su tutto il traffico in una qualsiasi delle interfacce del dispositivo.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 6. Selezionare il tipo di IP di origine appropriato a cui applicare la regola di accesso dall'elenco a discesa IP di origine.

- **Qualsiasi** - A qualsiasi indirizzo IP della rete del dispositivo è applicata la regola.
- **Singolo** — la regola viene applicata solo a un singolo indirizzo IP specificato sulla rete del dispositivo. Immettere l'indirizzo IP desiderato nel campo adiacente.
- **Intervallo** — Solo a un intervallo specificato di indirizzi IP sulla rete del dispositivo viene applicata la regola. Se si sceglie Intervallo, è necessario immettere il primo e l'ultimo indirizzo IP dell'intervallo nei campi adiacenti.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

Passaggio 7. Selezionare dall'elenco a discesa disponibile il tipo di IP di destinazione appropriato a cui applicare la regola di accesso.

- Qualsiasi - A qualsiasi indirizzo IP di destinazione è applicata la regola.
- Singolo — la regola viene applicata solo a un singolo indirizzo IP specificato. Immettere l'indirizzo IP desiderato nel campo adiacente.
- Intervallo - La regola viene applicata solo a un intervallo specificato di indirizzi IP esterni alla rete del dispositivo. Se si sceglie Intervallo, è necessario immettere il primo e l'ultimo indirizzo IP dell'intervallo nei campi adiacenti.

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Timesaver: Per impostazione predefinita, l'ora è impostata su Sempre. Se si desidera applicare la regola di accesso a un'ora o a un giorno specifico, seguire i passaggi da 8 a 11. In caso contrario,

andare al passaggio 12.

Passaggio 8. Scegliere **Intervallo** dall'elenco a discesa. Le regole di accesso sono attive per alcuni orari specifici. immettere l'intervallo di tempo per l'applicazione della regola di accesso.

Scheduling

Time: Interval

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Passaggio 9. Inserire l'ora in cui si desidera iniziare ad applicare l'elenco di accesso nel campo Da. Il formato dell'ora è hh:mm.

Passaggio 10. Inserire nel campo A l'ora in cui non si desidera più applicare l'elenco degli accessi. Il formato dell'ora è hh:mm.

Scheduling

Time: Interval

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Passaggio 11. Selezionare la casella di controllo dei giorni specifici in cui si desidera applicare l'elenco degli accessi.

Passaggio 12. Fare clic su **Save** per salvare le modifiche.

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 6 5

Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management... Page 1 of 2

Passaggio 13. (Facoltativo) Se si desidera ripristinare le regole predefinite, fare clic su **Ripristina regole predefinite**. Tutte le regole di accesso configurate dall'utente vengono perse.

Configurazione regola di accesso su IPv6

Access Rules

IPv4 **IPv6**

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Page 1 of 1

Passaggio 1. Fare clic sulla scheda IPv6 per configurare le regole di accesso IPv6.

Access Rules

IPv4 **IPv6**

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Page 1 of 1

Passaggio 2. Fare clic su Aggiungi per aggiungere una nuova regola di accesso IPv6. Viene visualizzata la finestra *Modifica regole di accesso*.

Edit Access Rules

Services

Action:

Service: [TCP&UDP/1~65535]

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Passaggio 3. Scegliere l'opzione appropriata dall'elenco a discesa Azione per consentire o limitare la regola da impostare. Le regole di accesso limitano l'accesso alla rete consentendo o negando l'accesso al traffico da servizi o dispositivi specifici.

- Consenti — consente tutto il traffico.
- Nega — limita tutto il traffico.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: **All Traffic [TCP&UDP/1~65535]**

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Save Cancel

All Traffic [TCP&UDP/1~65535]
 DNS [UDP/53~53]
 FTP [TCP/21~21]
 HTTP [TCP/80~80]
 HTTP Secondary [TCP/8080~8080]
 HTTPS [TCP/443~443]
 HTTPS Secondary [TCP/8443~8443]
 TFTP [UDP/69~69]
 IMAP [TCP/143~143]
 NNTP [TCP/119~119]
 POP3 [TCP/110~110]
 SNMP [UDP/161~161]
 SMTP [TCP/25~25]
 TELNET [TCP/23~23]
 TELNET Secondary [TCP/8023~8023]
 TELNET SSL [TCP/992~992]
 DHCP [UDP/67~67]
 L2TP [UDP/1701~1701]
 PPTP [TCP/1723~1723]
 IPSec [UDP/500~500]
 Ping [ICMP/255~255]
 data [TCP/520~521]

Passaggio 4. Scegliere il servizio appropriato da filtrare dall'elenco a discesa Servizio.

Nota: Per consentire tutto il traffico, scegliere **Tutto il traffico [TCP&UDP/1~65535]** dall'elenco a discesa dei servizi se l'azione è stata impostata su Consenti. L'elenco contiene tutti i tipi di servizi che è possibile filtrare.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: **No Log**

Source Interface: Enabled

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

Passaggio 5. Scegliere l'opzione Log appropriata dall'elenco a discesa Log. L'opzione log determina se il dispositivo manterrà un registro del traffico che corrisponde alle regole di accesso impostate.

- Abilitato - Consente al router di mantenere la registrazione dei log per il servizio selezionato.
- Not Log: disabilita il router per mantenere la traccia del log.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: LAN
WAN1
WAN2
ANY

Destination IP / Prefix Length:

Save Cancel Back

Passaggio 6. Fare clic sull'elenco a discesa Interfaccia e scegliere l'interfaccia di origine appropriata. In questa interfaccia viene applicata la regola di accesso.

- LAN: la regola di accesso influisce solo sul traffico LAN.
- WAN 1: la regola di accesso influenza solo il traffico WAN 1.
- WAN 2: la regola di accesso influenza solo il traffico WAN 2.
- Qualsiasi - La regola di accesso influisce su tutto il traffico in una qualsiasi delle interfacce del dispositivo.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: ANY ▾

Destination IP / Prefix Length: ANY
Single Subnet

Save Cancel Back

Passaggio 7. Selezionare il tipo di IP di origine appropriato a cui applicare la regola di accesso dall'elenco a discesa IP di origine/Lunghezza prefisso.

- ANY — A tutti i pacchetti ricevuti dalla rete del dispositivo viene applicata la regola.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Singolo — la regola viene applicata solo a un singolo indirizzo IP specificato nella rete del dispositivo. Immettere l'indirizzo IPv6 desiderato nel campo adiacente.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Subnet: la regola viene applicata solo agli indirizzi IP di una subnet. Immettere l'indirizzo di rete IPv6 e la lunghezza del prefisso della subnet desiderata nei campi adiacenti.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

- ANY
- Single
- Subnet

Save Cancel Back

Passaggio 8. Selezionare il tipo di IP di destinazione appropriato a cui applicare la regola di accesso dall'elenco a discesa IP di destinazione / Lunghezza prefisso.

- Qualsiasi - A qualsiasi indirizzo IP di destinazione è applicata la regola.
- Singolo — la regola viene applicata solo a un singolo indirizzo IP specificato sulla rete del dispositivo. Immettere l'indirizzo IPv6 desiderato.
- Subnet: la regola viene applicata solo agli indirizzi IP di una subnet. Immettere l'indirizzo di rete IPv6 e la lunghezza del prefisso della subnet desiderata nei campi adiacenti.

Passaggio 9. Per rendere effettive le modifiche, fare clic su **Salva**.

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

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