

Configurazione di una regola di accesso IPv4 sui router VPN RV016, RV042, RV042G e RV082

Obiettivo

Una regola di accesso consente al router di determinare, in base ai requisiti dell'utente, il traffico che può passare e il traffico che deve essere rifiutato attraverso il firewall. Ciò consente di aggiungere sicurezza al router.

Questo documento spiega la procedura per aggiungere o eliminare una regola di accesso sui router VPN RV016, RV042, RV042G e RV082.

Dispositivi interessati

- RV016
- RV042
- RV042G
- RV082

Versione del software

4.2.1.02

Gestisci regole di accesso IPv4

La pianificazione delle regole di accesso IPv4 è una configurazione facoltativa.

Aggiungi o elimina regole di accesso IPv4

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Firewall > Regole di accesso**. Viene visualizzata la pagina *Regole di accesso IPv4*. Fare clic su **Add**.



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN1	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN2	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Item 1-5 of 7 Rows per page : 5

Add Restore to Default Rules Page 1 of 2

Passaggio 2. Viene visualizzata la pagina *Servizio regole di accesso*. Nell'elenco a discesa Azione, scegliere **Consenti** per consentire il traffico. In caso contrario, scegliere **Nega** per negare il traffico.

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 3. Selezionare il servizio desiderato dall'elenco a discesa Servizio. Se il servizio appropriato non è disponibile, fare clic su **Gestione servizi**.

Nota: se il servizio desiderato è disponibile, andare al passo 6.

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.

Viene visualizzata una nuova finestra. Immettere un nome di servizio nel campo Nome servizio.

Service Name :

Protocol :

Port Range : to

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]

Passaggio 5. Selezionare il tipo di protocollo desiderato dall'elenco a discesa Protocollo.

- TCP (Transmission Control Protocol): protocollo del livello di trasporto utilizzato dalle applicazioni che richiedono una consegna garantita.
- UDP (User Datagram Protocol): utilizza socket di datagrammi per stabilire comunicazioni host-host. È più veloce di TCP, ma non ha la stessa probabilità di essere consegnato correttamente.
- IPv6 (Internet Protocol versione 6): indirizza il traffico Internet tra gli host in pacchetti instradati su reti specificate da indirizzi di routing.

Service Name :

Protocol : TCP ▼
TCP
UDP
IPv6 to

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]

Passaggio 6. Immettere l'intervallo di porte nei campi Intervallo porte. Questo intervallo dipende dal protocollo scelto.

Fare clic su **Aggiungi all'elenco**. Il Servizio verrà aggiunto all'elenco a discesa Servizio.

Altre opzioni includono **Elimina**, **Aggiorna** o **Aggiungi nuovo**.

Fare clic su **OK**. In questo modo la finestra viene chiusa e l'utente torna alla pagina *Servizio regole di accesso*.

Service Name :

Protocol :

Port Range : to

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]

Passaggio 7. Nell'elenco a discesa Registro, scegliere **Registra pacchetti corrispondenti a questa regola** per registrare i pacchetti in ingresso corrispondenti alla regola di accesso. In caso contrario, scegliere **Non registrare**.

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 8. Selezionare l'interfaccia interessata da questa regola dall'elenco a discesa Interfaccia di origine. L'interfaccia di origine è l'interfaccia dalla quale viene avviato il traffico.

- LAN: la LAN del router.
- WAN1: la rete geografica o la rete da cui il router ottiene Internet dall'ISP o dal router dell'hop successivo.
- WAN2: uguale a WAN1, con la differenza che si tratta di una rete secondaria.
- ANY - Consente di utilizzare qualsiasi interfaccia.

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 9. Nell'elenco a discesa Source IP (IP origine), scegliere un'opzione per specificare l'intervallo di indirizzi IP di origine che l'interfaccia deve consentire o negare. I pacchetti che arrivano sull'interfaccia vengono verificati dall'IP di origine e di destinazione.

- Qualsiasi: la regola di accesso verrà applicata a tutto il traffico proveniente dall'interfaccia di origine. Non sono disponibili campi a destra dell'elenco a discesa.
- Singola: la regola di accesso verrà applicata a un singolo indirizzo IP dall'interfaccia di origine. Immettere l'indirizzo IP desiderato nel campo indirizzo.
- Intervallo: la regola di accesso verrà applicata a una rete subnet dall'interfaccia di origine. Immettere l'indirizzo IP e la lunghezza del prefisso.

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 9. Nell'elenco a discesa Destinazione, scegliere un'opzione per specificare l'intervallo di indirizzi di destinazione che devono essere consentiti o negati dall'interfaccia. I pacchetti che arrivano sull'interfaccia vengono verificati dall'IP di origine e di destinazione.

- **Qualsiasi:** la regola di accesso verrà applicata a tutto il traffico diretto all'interfaccia di destinazione. Non sono disponibili campi a destra dell'elenco a discesa.
- **Singola:** la regola di accesso verrà applicata su un singolo indirizzo IP all'interfaccia di destinazione. Immettere l'indirizzo IP desiderato nel campo indirizzo.
- **Intervallo:** la regola di accesso verrà applicata su una rete subnet all'interfaccia di destinazione. Immettere l'indirizzo IP e la lunghezza del prefisso.

Fare clic su **Salva** per salvare tutte le modifiche apportate alla regola di accesso. Viene visualizzata una finestra di conferma che fornisce lo stato delle modifiche apportate sul dispositivo.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 10. Fare clic su **OK** per aggiungere un'altra regola di accesso. Fare clic su **Annulla** per tornare alla pagina *Regole di accesso*.

Settings are successful. Press 'OK' to add another access rule, or press 'Cancel' to return to the page of Access Rules.

Passaggio 11 (facoltativo). Selezionare la regola di accesso desiderata dall'elenco e quindi fare clic su **Pulsante Modifica** per modificare la configurazione della regola di accesso.

Access Rules

IPv4



Item 1-5 of 5 Rows per page : 5

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		<input checked="" type="checkbox"/> <input type="button" value="Edit"/>
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Page 1 of 1

Passaggio 12 (facoltativo). Selezionare le regole di accesso desiderate dall'elenco e quindi fare clic su



Pulsante Elimina per eliminare la regola di accesso dall'elenco delle regole di accesso.

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	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		

Pianifica regole di accesso IPv4



La pianificazione delle regole di accesso consente di specificare una pianificazione in base alla quale queste regole di accesso sono attive in termini di giorno e ora. Funziona solo con IPv4.

Passaggio 1. Usare l'utility di configurazione Web e scegliere **Firewall > Regole di accesso**. Viene visualizzata la pagina *Regole di accesso IPv4*:

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	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		

Passaggio 2. Scegliere la regola di accesso dalla tabella e fare clic sull'icona **Modifica** per aggiungere la funzionalità di pianificazione a tale regola di accesso.

Nota: quando si aggiunge una nuova regola di accesso, è anche possibile aggiungere la funzionalità di pianificazione.

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	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		

Passaggio 3. Scegliere l'ora dall'elenco a discesa Ora. Specifica quando utilizzare la programmazione.

- Sempre: la regola di accesso si applica in ogni momento e in tutti i giorni della settimana. Per impostazione predefinita, è selezionata. Se si sceglie questa opzione, fare clic su *Save* (Salva) per andare al passaggio 6.
- Intervallo - In base all'intervallo di tempo specificato dall'utente, viene applicata la regola di accesso.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 4. Immettere l'intervallo di tempo nel formato 24 ore durante il quale la regola di accesso viene applicata nei campi *Da* e *A*.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 5. Selezionare le caselle di controllo accanto ai giorni ai quali si desidera applicare la regola di accesso. La regola di accesso sarà valida solo nei giorni selezionati. Per impostazione predefinita, è selezionato *Everyday* (Tutti i giorni).

Fare clic su **Salva** per salvare tutte le modifiche apportate alla regola di accesso. Viene visualizzata una finestra di conferma che fornisce lo stato delle modifiche apportate sul dispositivo.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Passaggio 6. Fare clic su **OK** per aggiungere un'altra regola di accesso. Fare clic su **Annulla** per tornare alla pagina delle regole di accesso.

Settings are successful. Press 'OK' to add another access rule, or press 'Cancel' to return to the page of Access Rules.

Conclusioni

A questo punto, è necessario configurare le regole di accesso IPv4 sul router VPN RV016, RV042, RV042G o RV082.

Se si desidera accedere a tutti i servizi di supporto per questi router, consultare la pagina del prodotto facendo clic [qui](#).

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).