Configurazione di una regola di accesso IPv6 su router VPN RV016, RV042, RV042G e RV082

Obiettivo

Una regola di accesso consente al router di determinare il traffico che può passare attraverso il firewall. Ciò consente di aggiungere sicurezza al router.

In questo articolo viene illustrato come aggiungere una regola di accesso IPv6 ai router VPN RV016, RV042, RV042G e RV082.

Dispositivi interessati

· RV016
RV042
RV042G
RV082

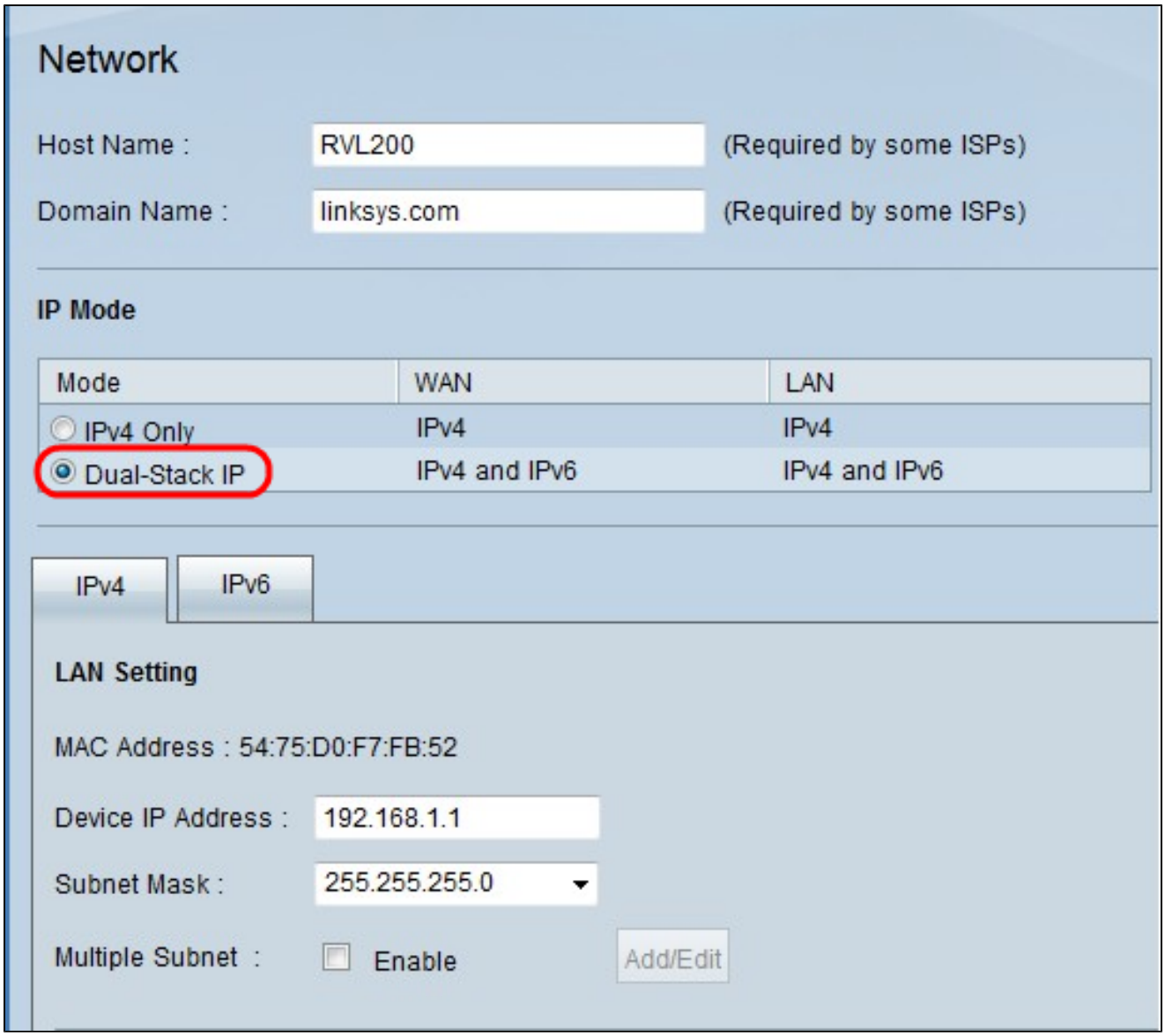
Versione del software

· v4.2.1.02

Configurazione di una regola di accesso IPv6

Abilita modalità IPv6

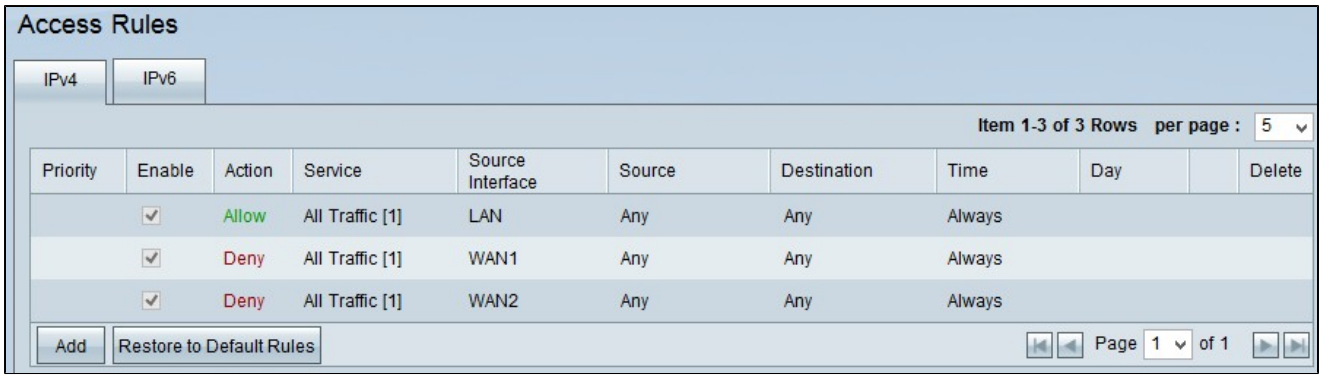
Passaggio 1. Accedere all'utility di configurazione Web e scegliere Impostazione > Rete. Viene visualizzata la pagina Rete:



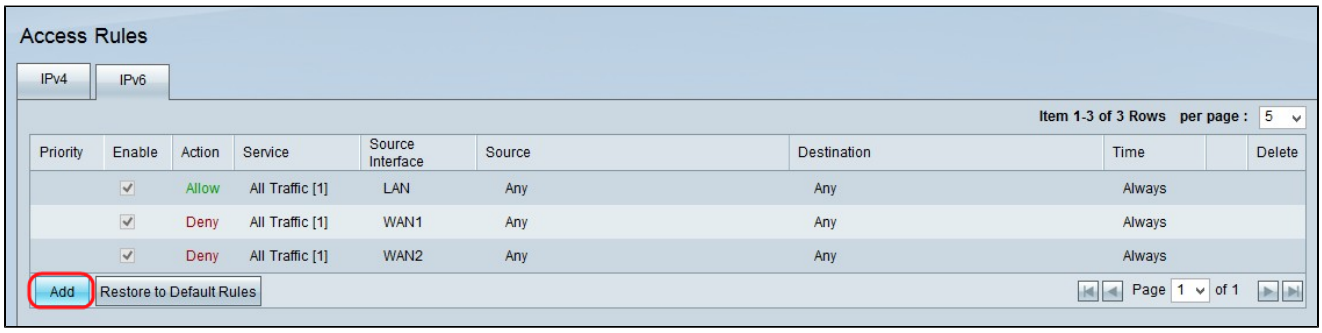
Passaggio 2. Fare clic sul pulsante di opzione Dual-Stack IP. Ciò consente l'esecuzione simultanea di IPv4 e IPv6. Se la comunicazione IPv6 è possibile, questa è la comunicazione preferita.

Configurazione regola di accesso IPv6

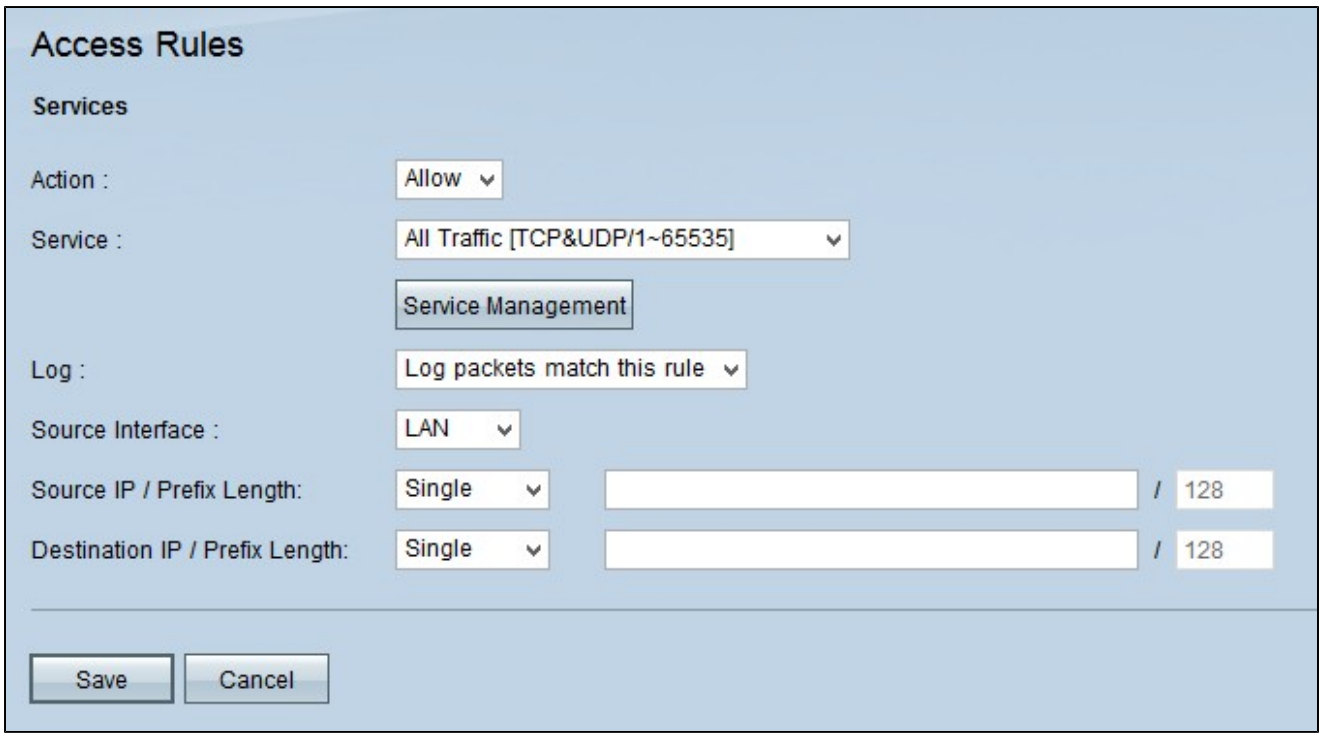
Passaggio 1. Accedere all'utility di configurazione Web e scegliere Firewall > Regole di accesso. Viene visualizzata la pagina Regole di accesso:



Passaggio 2. Fare clic sulla scheda IPv6. Verrà aperta la pagina Regole di accesso IPv6.



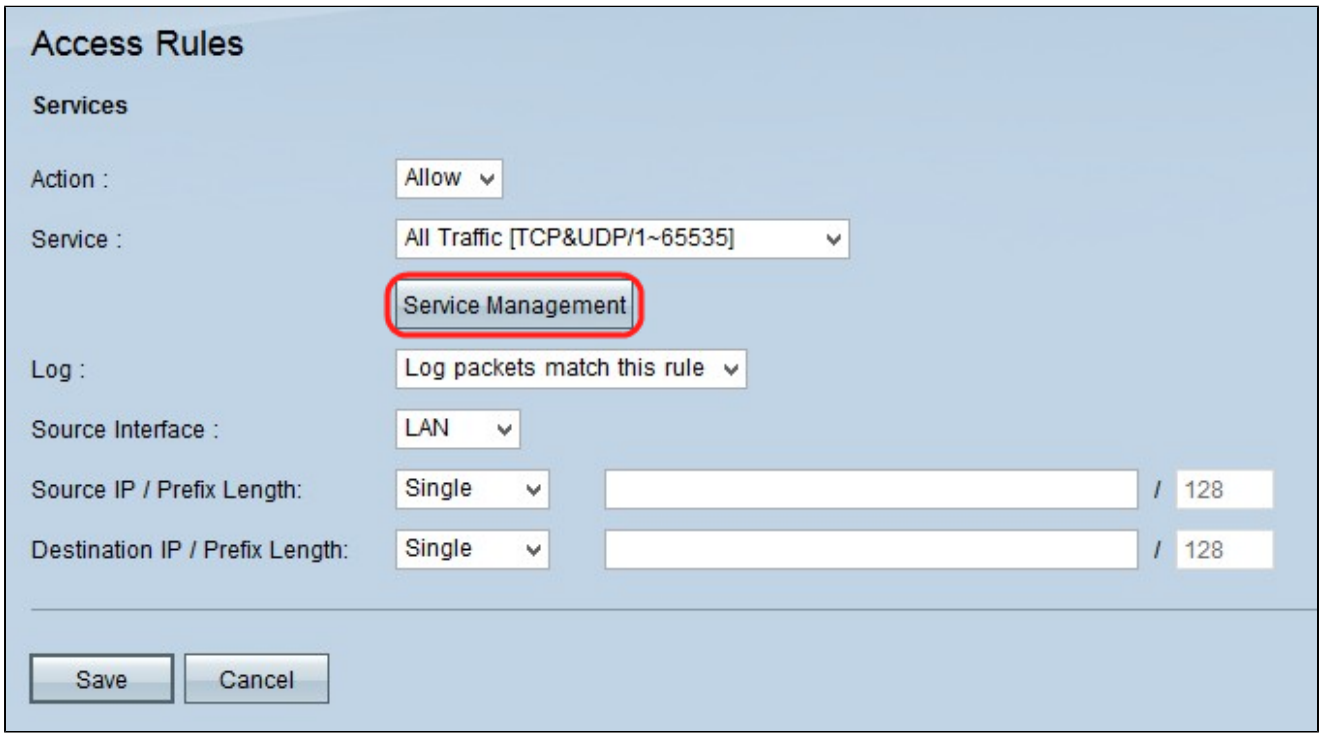
Passaggio 3. Fare clic su Add per aggiungere le regole di accesso. Viene visualizzata la pagina Regole di accesso per configurare le regole di accesso per IPv6.



Passaggio 4. Per consentire il traffico, selezionare Allow (Consenti) dall'elenco a discesa Action (Azione). Scegliere Nega per negare il traffico.

Passaggio 5. Scegliere il servizio appropriato dall'elenco a discesa Servizio.

Timesaver: se il servizio desiderato è disponibile, passare al punto 12.



Passaggio 6. Se il servizio appropriato non è disponibile, fare clic su Gestione servizi. Viene visualizzata la finestra Gestione assistenza.

Service Name :

Protocol : TCP

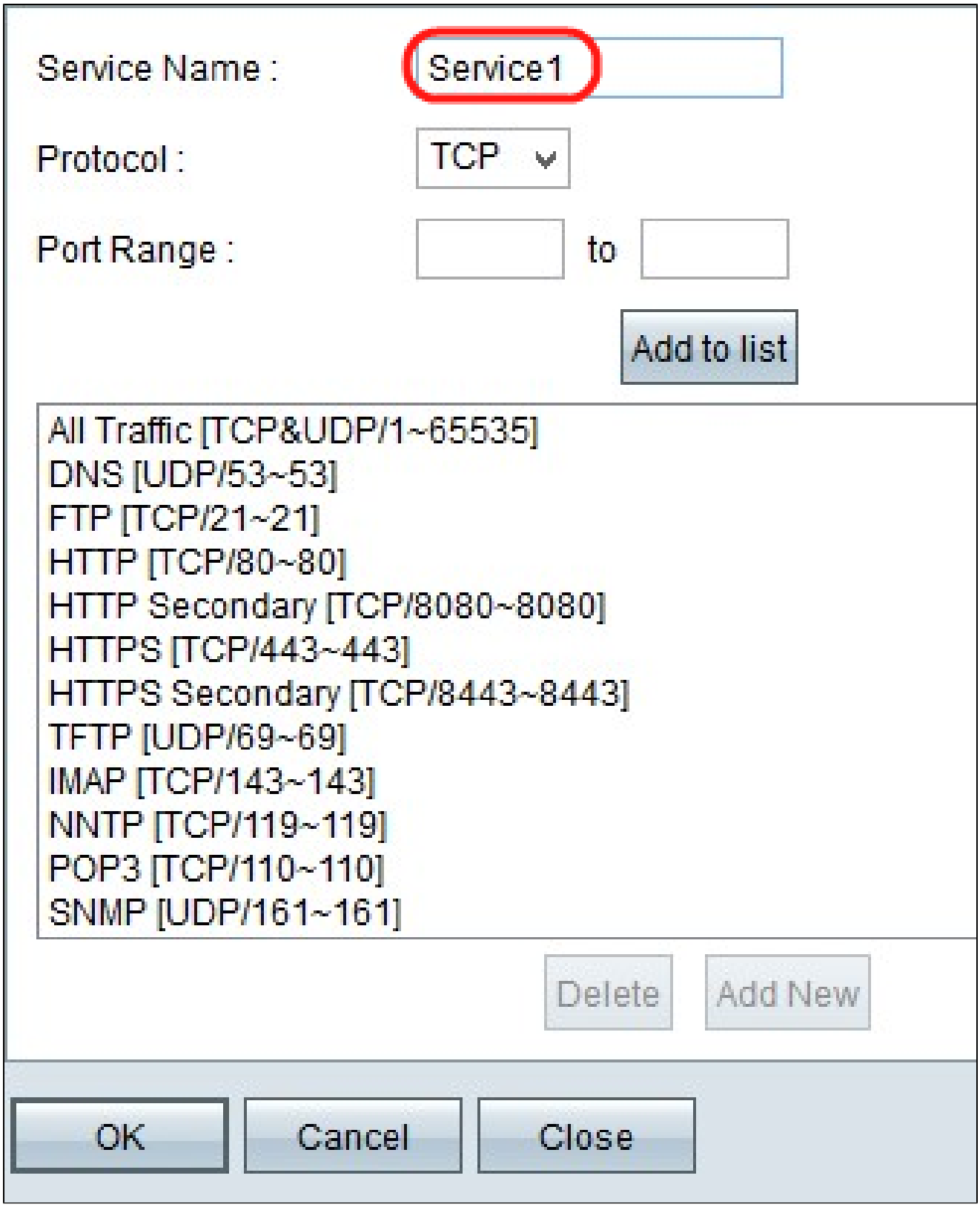
Port Range : to

Add to list

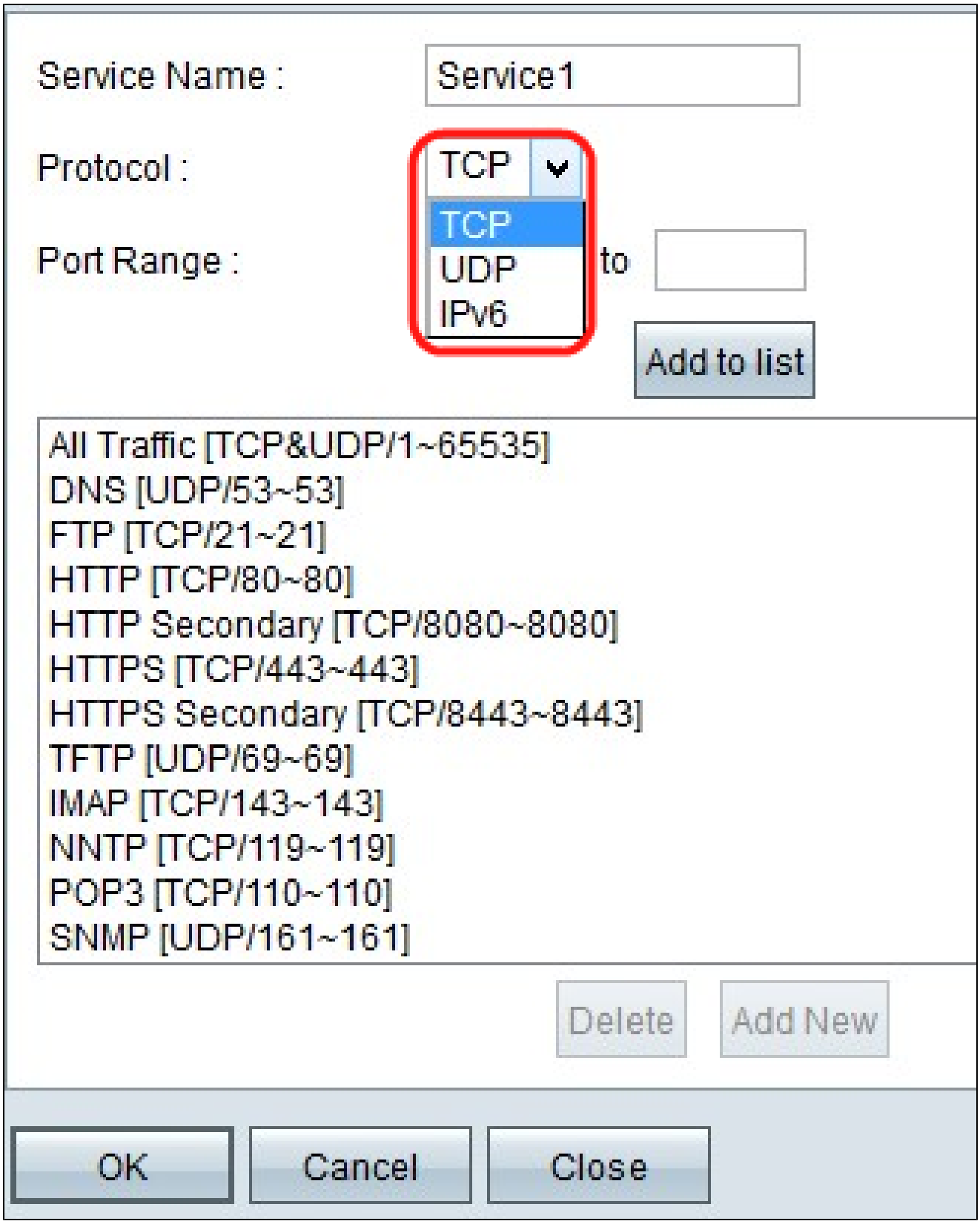
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Delete Add New

OK Cancel Close



Passaggio 7. Immettere un nome per il nuovo servizio nel campo Nome servizio.

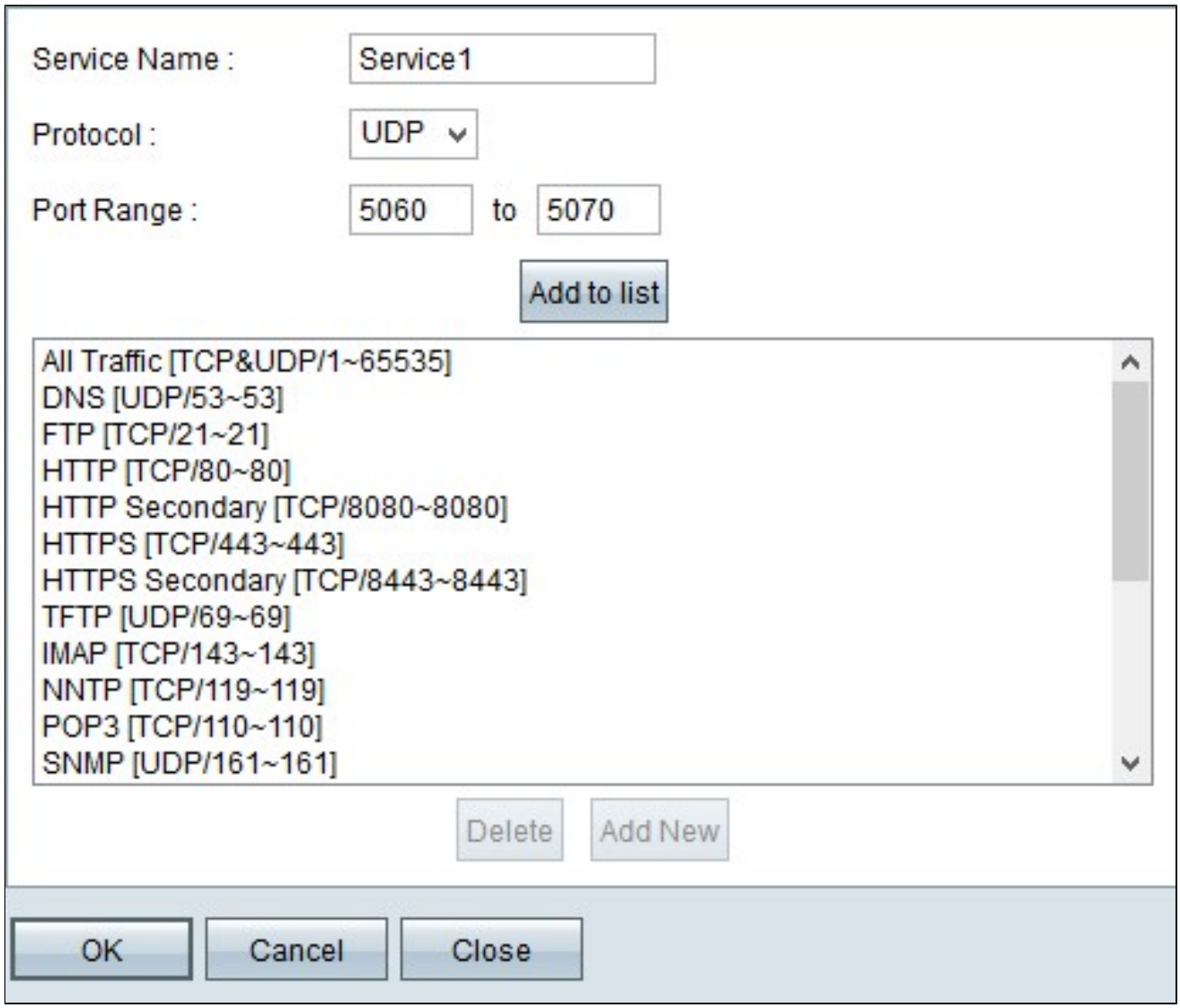


Passaggio 8. Selezionare il tipo di protocollo desiderato dall'elenco a discesa Protocollo.

· TCP (Transmission Control Protocol): protocollo del livello di trasporto utilizzato dalle applicazioni che richiede una consegna garantita.

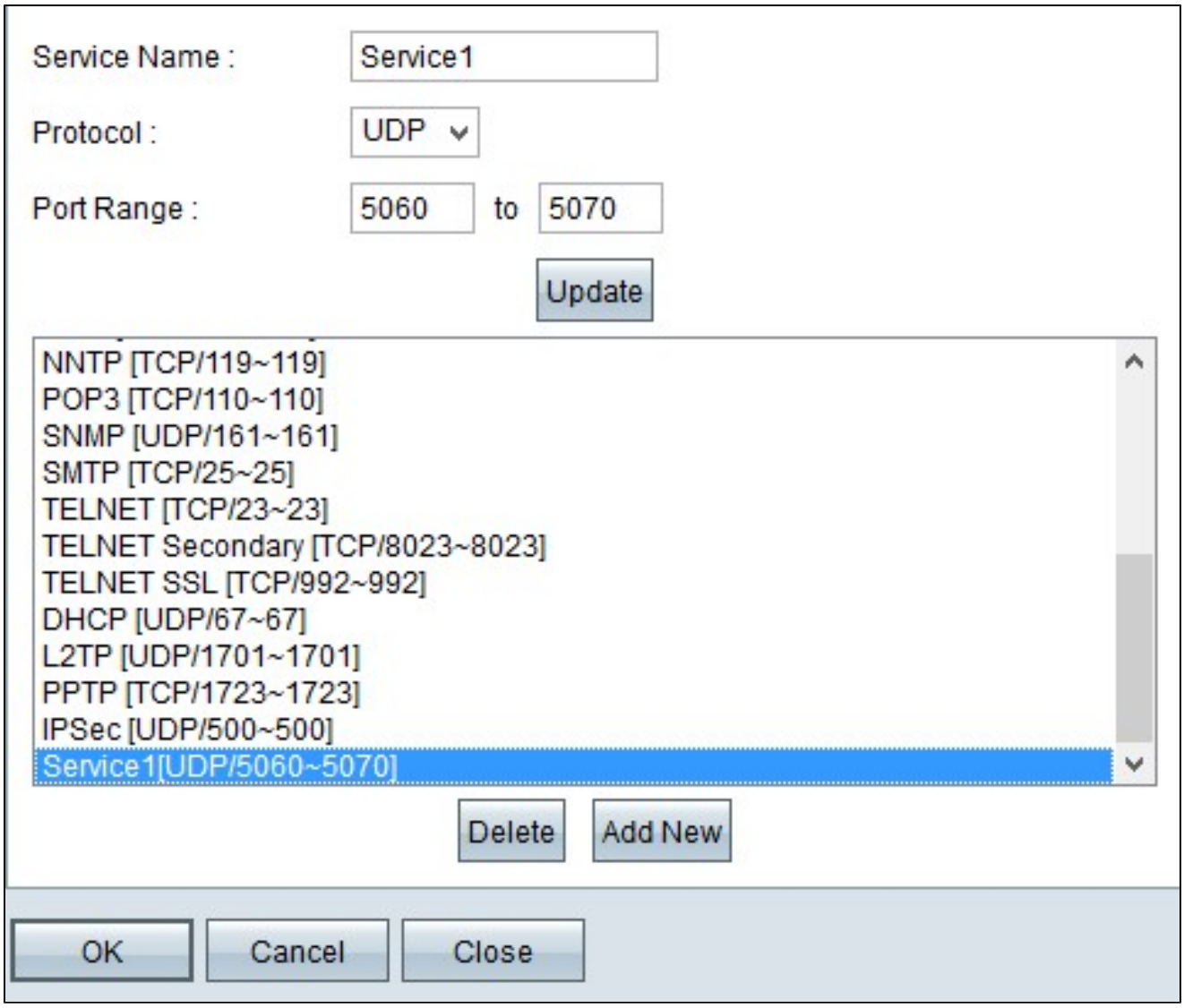
· UDP (User Datagram Protocol): utilizza socket di datagrammi per stabilire comunicazioni host-host. Il recapito UDP non è garantito.

· IPv6 (Internet Protocol versione 6): indirizza il traffico Internet tra gli host in pacchetti instradati su reti specificate da indirizzi di routing.



Passaggio 9. Immettere l'intervallo di porte nel campo Intervallo porte. Questo intervallo dipende dal protocollo scelto nel passaggio precedente.

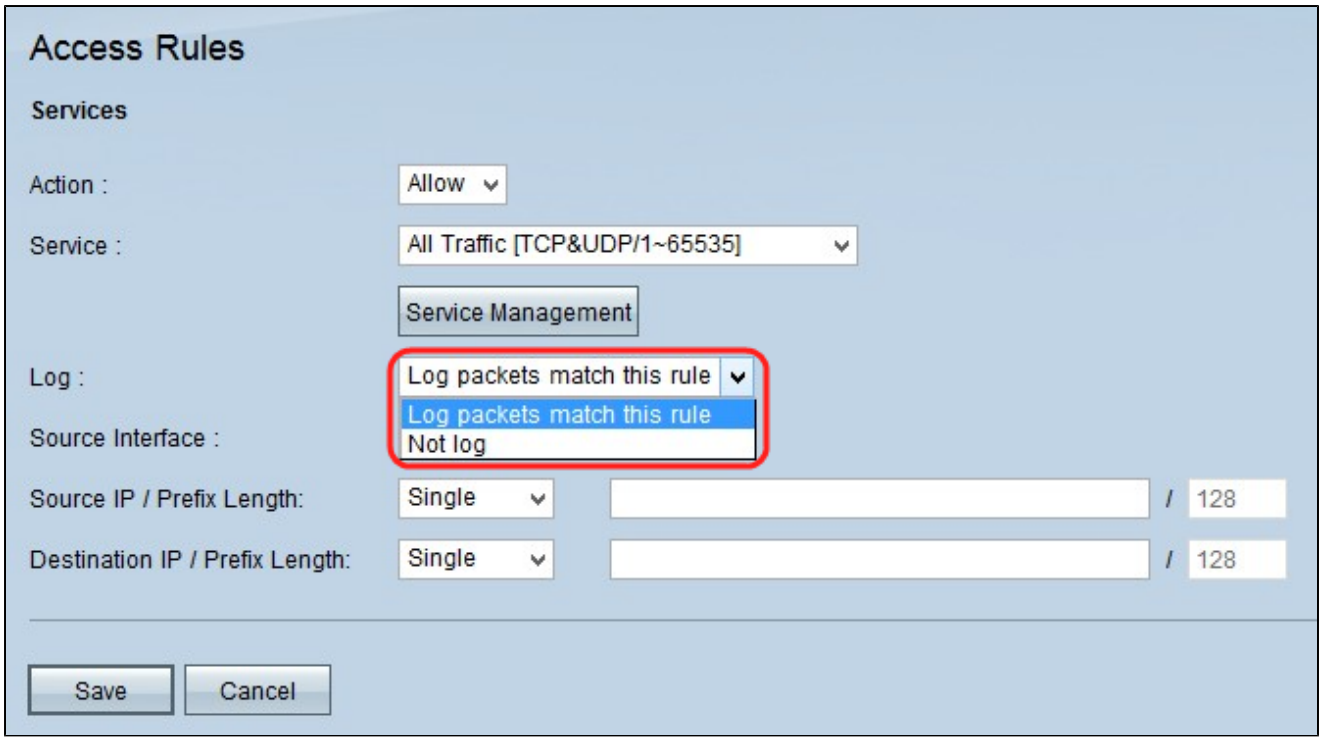
Passaggio 10. Fare clic su Aggiungi all'elenco. Il Servizio verrà aggiunto all'elenco a discesa Servizio.



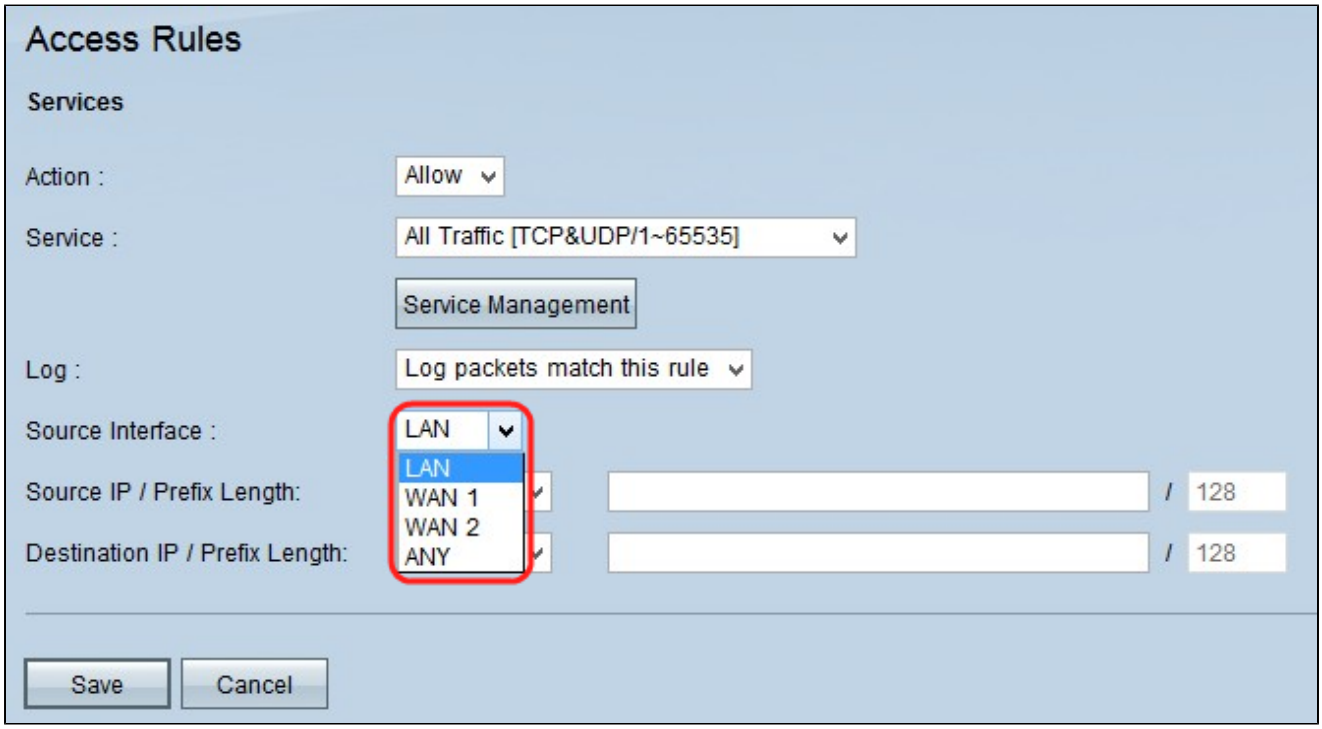
Nota: se si desidera eliminare il servizio dall'elenco dei servizi, selezionarlo dall'elenco dei servizi e fare clic su Elimina. Se si desidera aggiornare la voce relativa al servizio, scegliere il servizio da aggiornare dall'elenco dei servizi e quindi fare clic su Aggiorna. Per aggiungere un altro nuovo servizio all'elenco, fare clic su Aggiungi nuovo.

Passaggio 11. Fare clic su OK. In questo modo la finestra viene chiusa e l'utente torna alla pagina Regola di accesso.

Nota: se fate clic su Aggiungi nuovo (Add New), seguite i passi da 7 a 11.



Passaggio 12. Se si desidera registrare i pacchetti che soddisfano la regola di accesso, scegliere Registra i pacchetti che soddisfano questa regola nell'elenco a discesa Registro. In caso contrario, scegliere Non registrare.



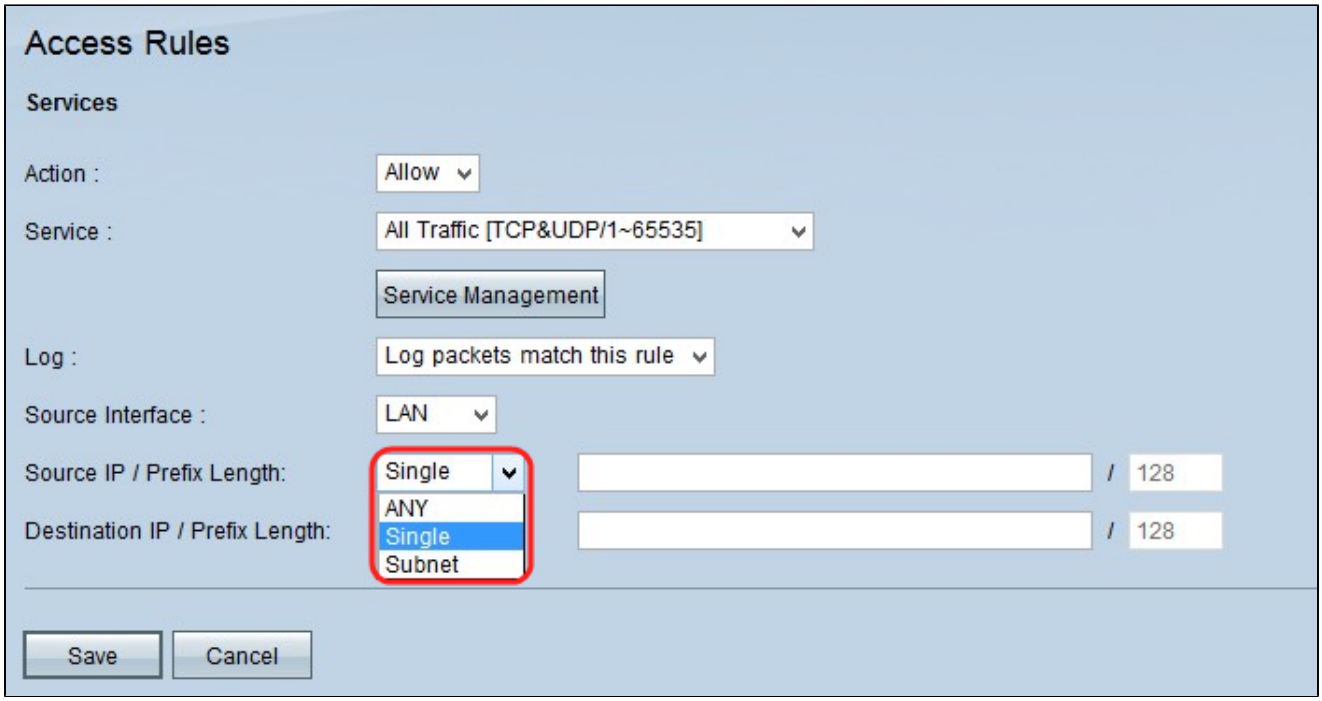
Passaggio 13. Selezionare l'interfaccia interessata da questa regola dall'elenco a discesa Interfaccia di origine. L'interfaccia di origine è l'interfaccia dalla quale viene avviato il traffico.

· 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.

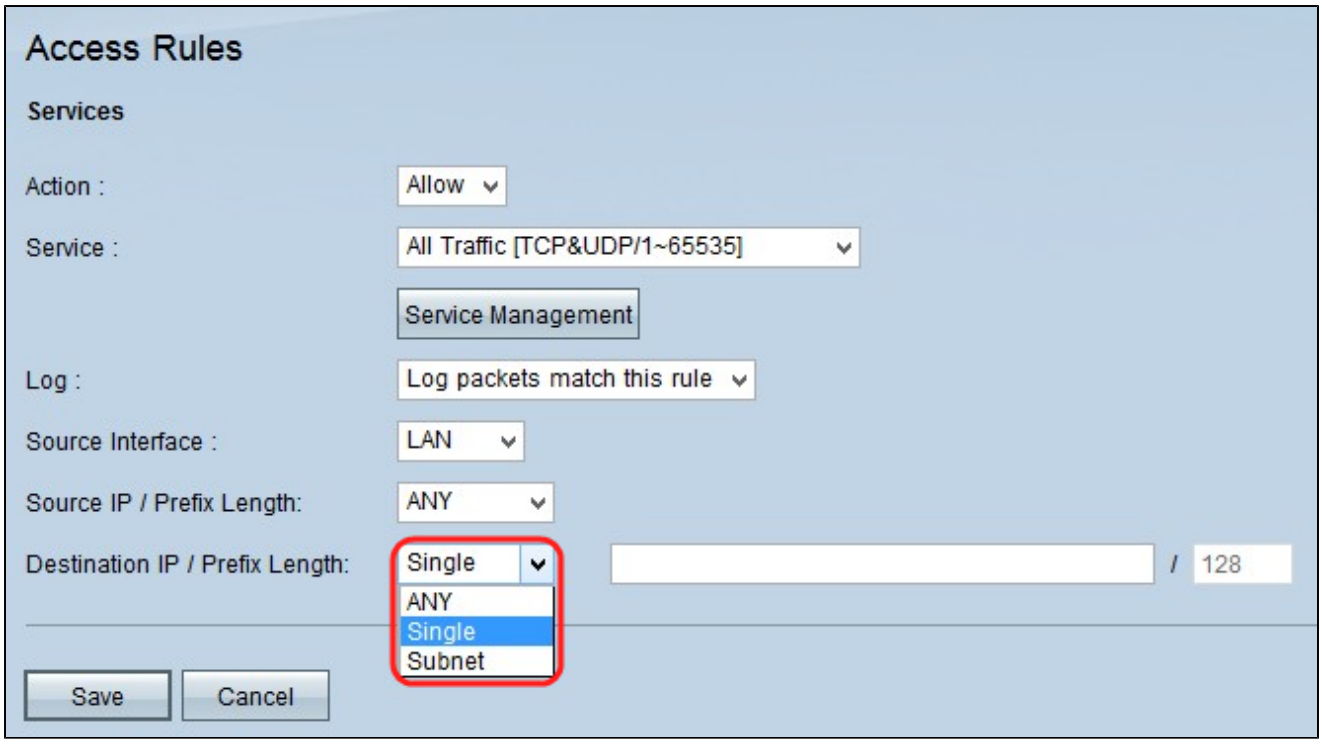


Passaggio 14. Nell'elenco a discesa Source IP (IP di origine), scegliere un'opzione per specificare l'indirizzo IP di origine a cui applicare la regola di accesso.

· 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.

· Subnet: la regola di accesso verrà applicata a una rete subnet dall'interfaccia di origine. Immettere l'indirizzo IP e la lunghezza del prefisso.



Passaggio 15. Nell'elenco a discesa IP di destinazione selezionare un'opzione per specificare l'indirizzo IP di destinazione a cui applicare la regola di accesso.

· 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.

· Subnet: la regola di accesso verrà applicata a una rete subnet all'interfaccia di destinazione. Immettere l'indirizzo IP e la lunghezza del prefisso.

Passaggio 16. Fare clic su Salva per salvare tutte le modifiche apportate alla regola di accesso IPv6.

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).