Risoluzione dei problemi relativi agli elenchi degli accessi sulla rete privata virtuale sui router VPN RV016, RV042, RV042G e RV082

Obiettivi

Un elenco di controllo di accesso (ACL, Access Control List) è una raccolta di condizioni di autorizzazione e rifiuto. Un ACL specifica a quali utenti o processi di sistema è concesso l'accesso a risorse specifiche. Un ACL può bloccare qualsiasi tentativo non giustificato di raggiungere le risorse di rete. Il problema in questa situazione può verificarsi quando gli ACL sono configurati su entrambi i router, ma uno dei router non può distinguere tra gli elenchi di traffico autorizzato e non autorizzato dall'ACL. Zenmap, uno strumento open source utilizzato per verificare il tipo di filtri/firewall attivi, viene usato per testare la configurazione.

Questo articolo spiega come risolvere i problemi relativi agli ACL consentiti che non funzionano sulla VPN da gateway a gateway tra due router VPN.

Dispositivi interessati

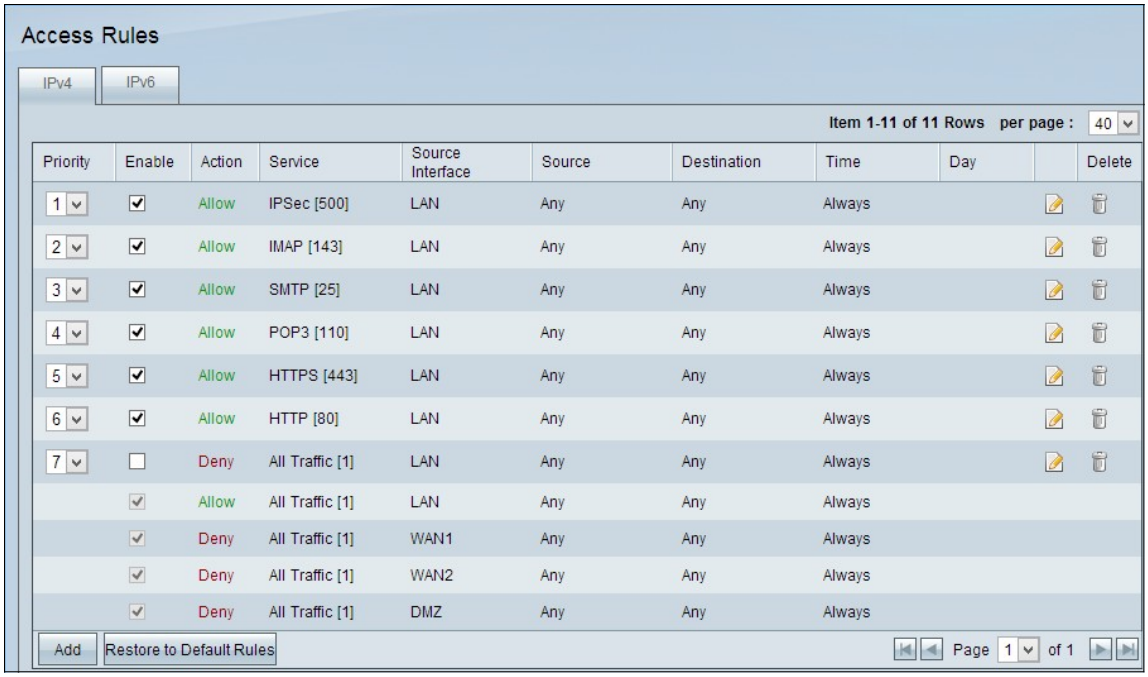
RV016
RV042
RV042G
RV082

Versione del software

·v4.2.2.08

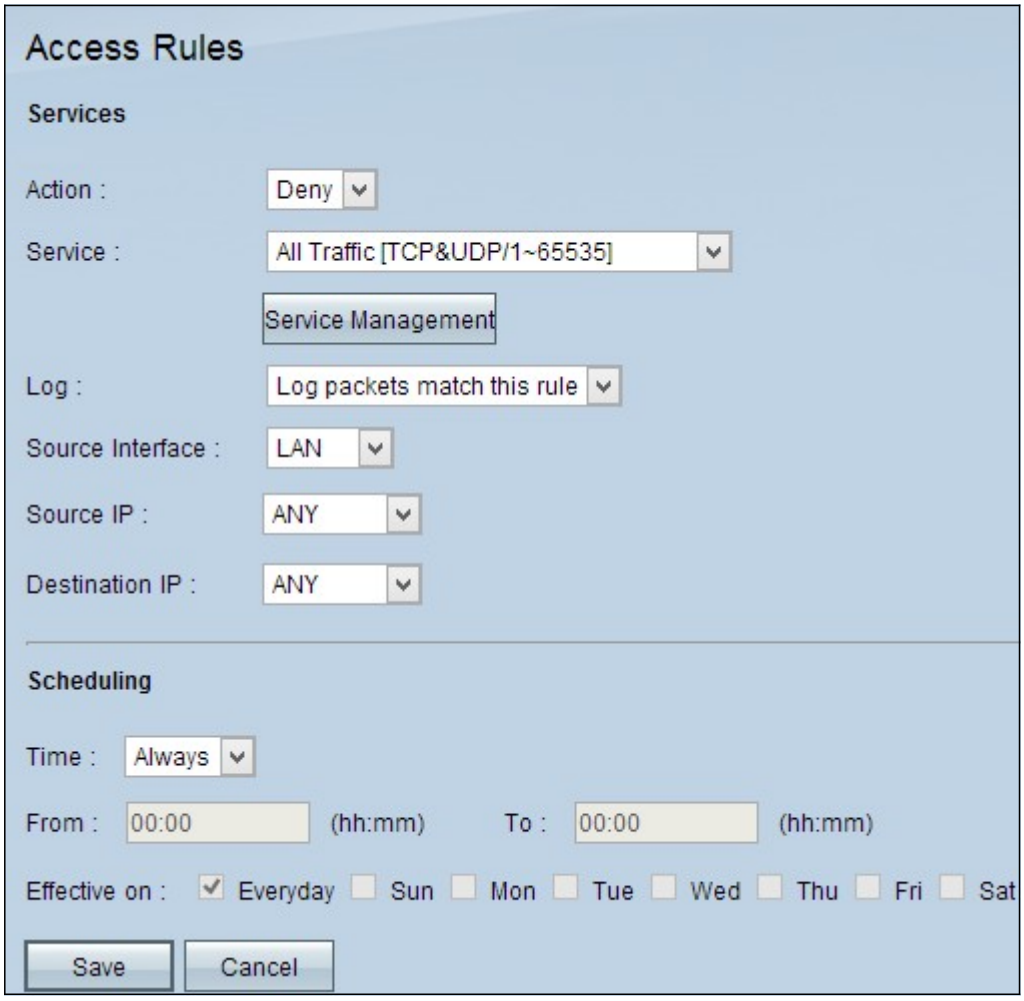
Configurazione ACL over VPN

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

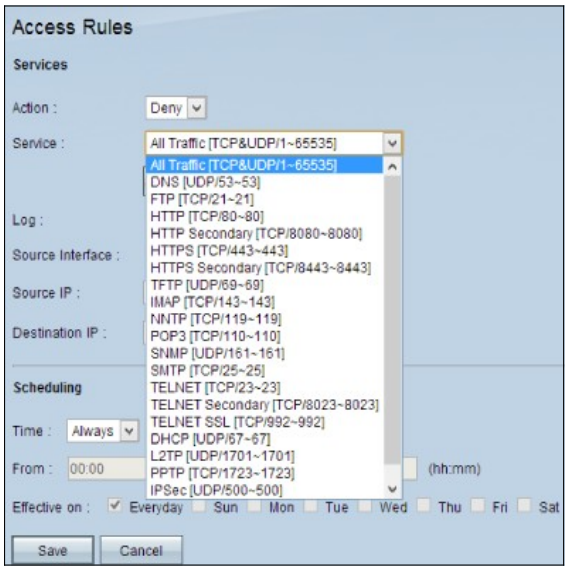


Nota: Impossibile modificare le regole di accesso predefinite. Le regole di accesso menzionate nell'immagine sopra configurate dall'utente possono essere modificate nel modo seguente.

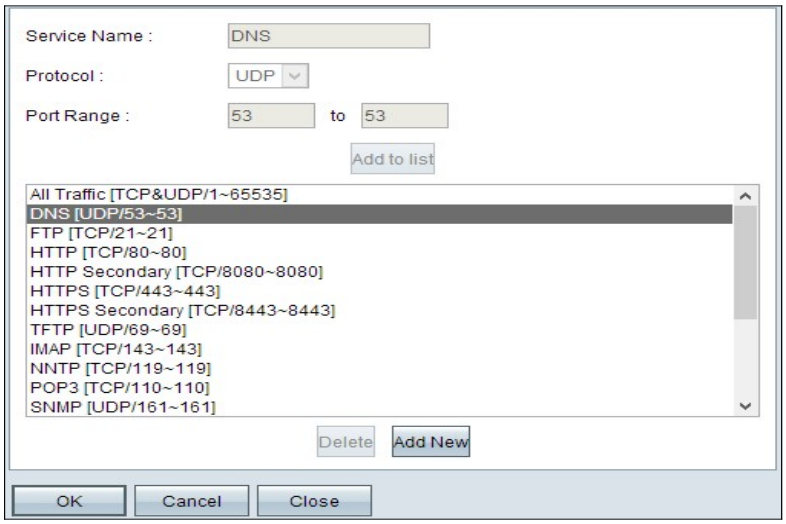
Passaggio 2. Fare clic sul pulsante **Aggiungi** per aggiungere una nuova regola di accesso. La pagina *Regole di accesso* cambia per visualizzare le aree Servizi e Pianificazione. L'aggiunta di una regola di accesso viene illustrata nei passaggi seguenti.



Passaggio 3. Scegliere **Nega** dall'elenco a discesa Azione per negare il servizio.



Passaggio 4. Scegliere il servizio richiesto da applicare alla regola dall'elenco a discesa **Servizio**.



Passaggio 5. (Facoltativo) Per aggiungere un servizio non presente nell'elenco a discesa Servizio, fare clic su **Gestione servizio**. In Gestione servizi è possibile creare un servizio in base alle esigenze. Dopo aver creato un servizio, fare clic su **OK** per salvare le impostazioni.

Passaggio 6. Scegliere **Registra i pacchetti che soddisfano questa regola** dall'elenco a discesa Registra solo per i registri che soddisfano o **Non registra** per i registri che non soddisfano la regola di accesso.

Passaggio 7. Scegliere un tipo di interfaccia dall'elenco a discesa Interfaccia di origine che rappresenta l'origine delle regole di accesso. Le opzioni disponibili sono:

·LAN: selezionare LAN se l'interfaccia di origine è Local Area Network.

·WAN: scegliere WAN se l'interfaccia di origine è l'ISP.

·DMZ - Scegliere DMZ se l'interfaccia di origine è la zona demilitarizzata.

·ANY - Scegliere ANY per impostare l'interfaccia di origine come una delle interfacce sopra menzionate.

Passaggio 8. Dall'elenco a discesa Source IP (IP origine), scegliere gli indirizzi di origine desiderati da applicare alla regola di accesso. Le opzioni disponibili sono:

·Singolo: scegliere Singolo se si tratta di un singolo indirizzo IP e immettere l'indirizzo IP.

·Intervallo: scegliere Intervallo se si tratta di un intervallo di indirizzi IP e immettere il primo e l'ultimo indirizzo IP dell'intervallo.

·ANY (QUALSIASI) - Consente di applicare le regole a tutti gli indirizzi IP di origine.

Passaggio 9. Dall'elenco a discesa IP di destinazione, scegliere gli indirizzi di destinazione desiderati da applicare alla regola di accesso. Le opzioni disponibili sono:

·Singolo: scegliere Singolo se si tratta di un singolo indirizzo IP e immettere l'indirizzo IP.

·Intervallo: scegliere Intervallo se si tratta di un intervallo di indirizzi IP e immettere il primo e l'ultimo indirizzo IP dell'intervallo.

·ANY (QUALSIASI) - Consente di applicare le regole a tutti gli indirizzi IP di destinazione.

Passaggio 10. Scegliere un metodo per definire quando le regole sono attive dall'elenco a discesa Ora. più di un'opzione:

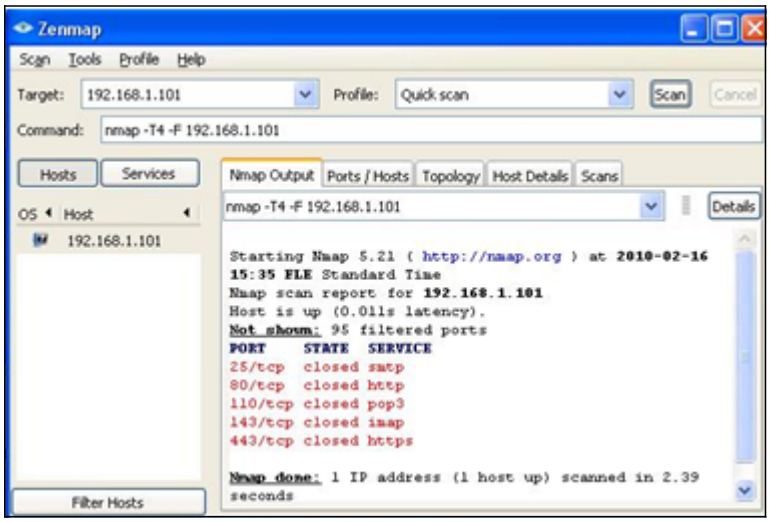
·Sempre: se si sceglie Sempre dall'elenco a discesa Ora, le regole di accesso vengono sempre applicate al traffico.

· Intervallo: se si seleziona Intervallo dall'elenco a discesa Tempo, è possibile scegliere un intervallo di tempo specifico per l'attivazione delle regole di accesso. Dopo aver specificato l'intervallo di tempo, selezionare le caselle di controllo dei giorni in cui si desidera che le regole di accesso siano attive nel campo Validità il.

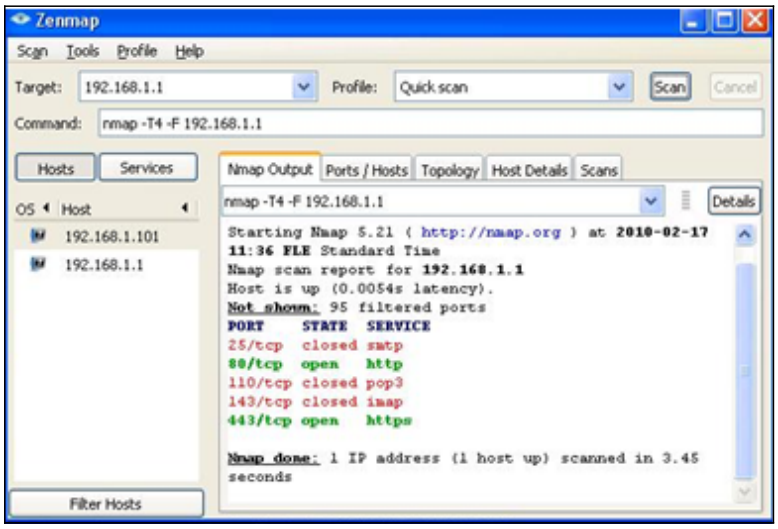
Passaggio 11. Fare clic su **Save** per salvare le impostazioni.

Passaggio 12. Ripetere i passaggi da 2 a 10 con i campi corrispondenti a quelli visualizzati rispettivamente nell'immagine. Le regole di accesso in base al cliente vengono applicate qui. I primi 7 stanno permettendo alcuni servizi; l'8 nega tutto il resto del traffico. Questa configurazione viene eseguita anche sul secondo router. Porta IPSec 500 consentita.

Nota: Eseguire questa operazione su entrambi i router per verificare che le regole di accesso siano configurate come desiderato.



VPN Router n. 1

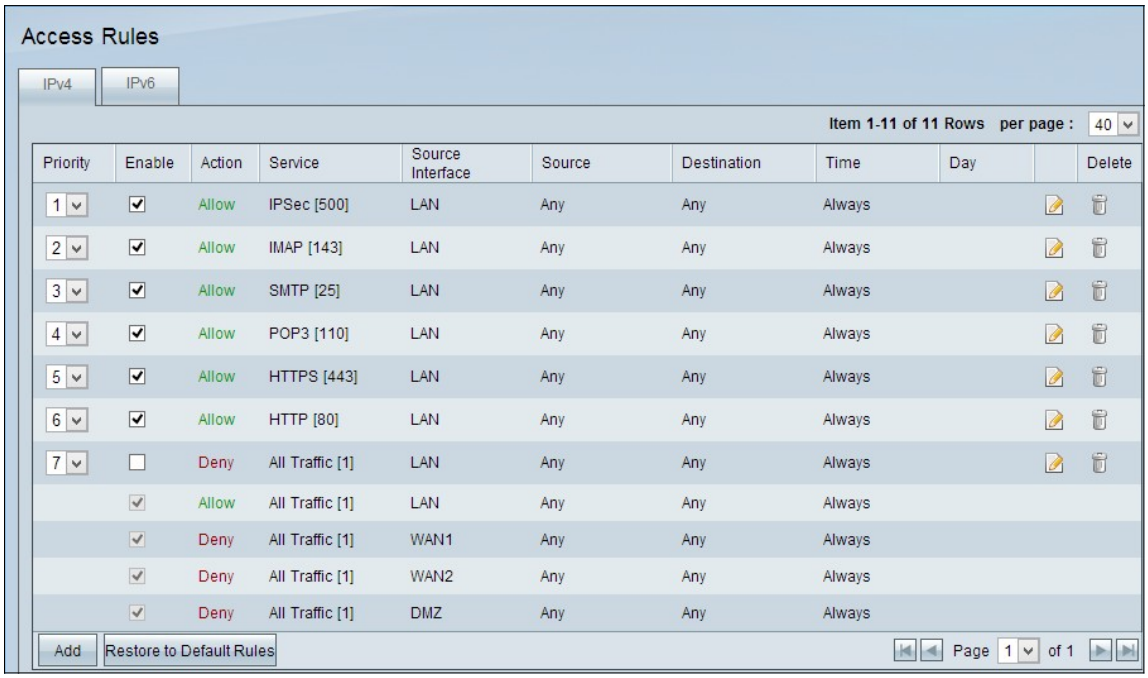


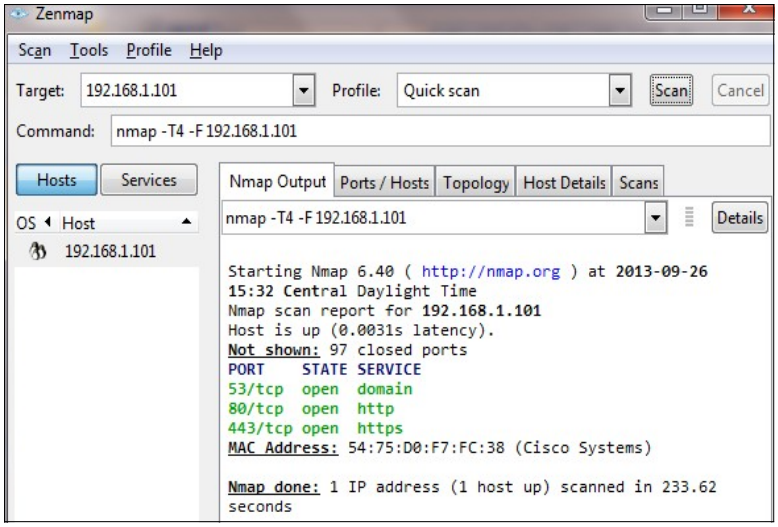
VPN Router n. 2

Passaggio 13. Installare Zenmap(NMAP) da http://nmap.org/download.html e avviarlo su un PC nella LAN 192.168.2.0.

Nota: Questa è la LAN dietro il router con i sette ACL aggiuntivi. L'IP di destinazione (192.168.1.101) è un PC sulla LAN del gateway remoto.

Passaggio 14. Selezionare **Analisi veloce** dal profilo e fare clic su **Scansione**. Tramite questa procedura, possiamo conoscere le porte aperte e filtrate in base agli ACL, e il risultato mostrato è rappresentato nell'immagine precedente. L'output mostra che queste porte sono chiuse, a prescindere dagli ACL consentiti configurati sulla RV0xx # 1. Se si tenta di controllare le porte sull'indirizzo IP LAN (192.168.1.1) del gateway remoto, le porte 80 e 443 sono aperte (chiuse sul PC 192.168.1.101).





L'ACL funziona correttamente dopo la rimozione del 7° ACL rifiutato e funziona correttamente come si può vedere dall'output.

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).