Configurazione dei profili di accesso sugli switch gestiti serie 200/300

Obiettivo

I profili di accesso fungono da altro livello di protezione per lo switch. I profili di accesso possono contenere fino a 128 regole per aumentare la protezione. Ogni regola contiene un'azione e un criterio. Se il metodo di accesso non corrisponde al metodo di gestione, all'utente viene impedito di accedere al dispositivo.

In questo documento viene spiegato come configurare i profili per accedere agli switch gestiti serie 200/300.

Dispositivi interessati

· SF/SG serie 200 e SF/SG serie 300 Managed Switch

Versione del software

•1.3.0.62

Configurazione profili di accesso

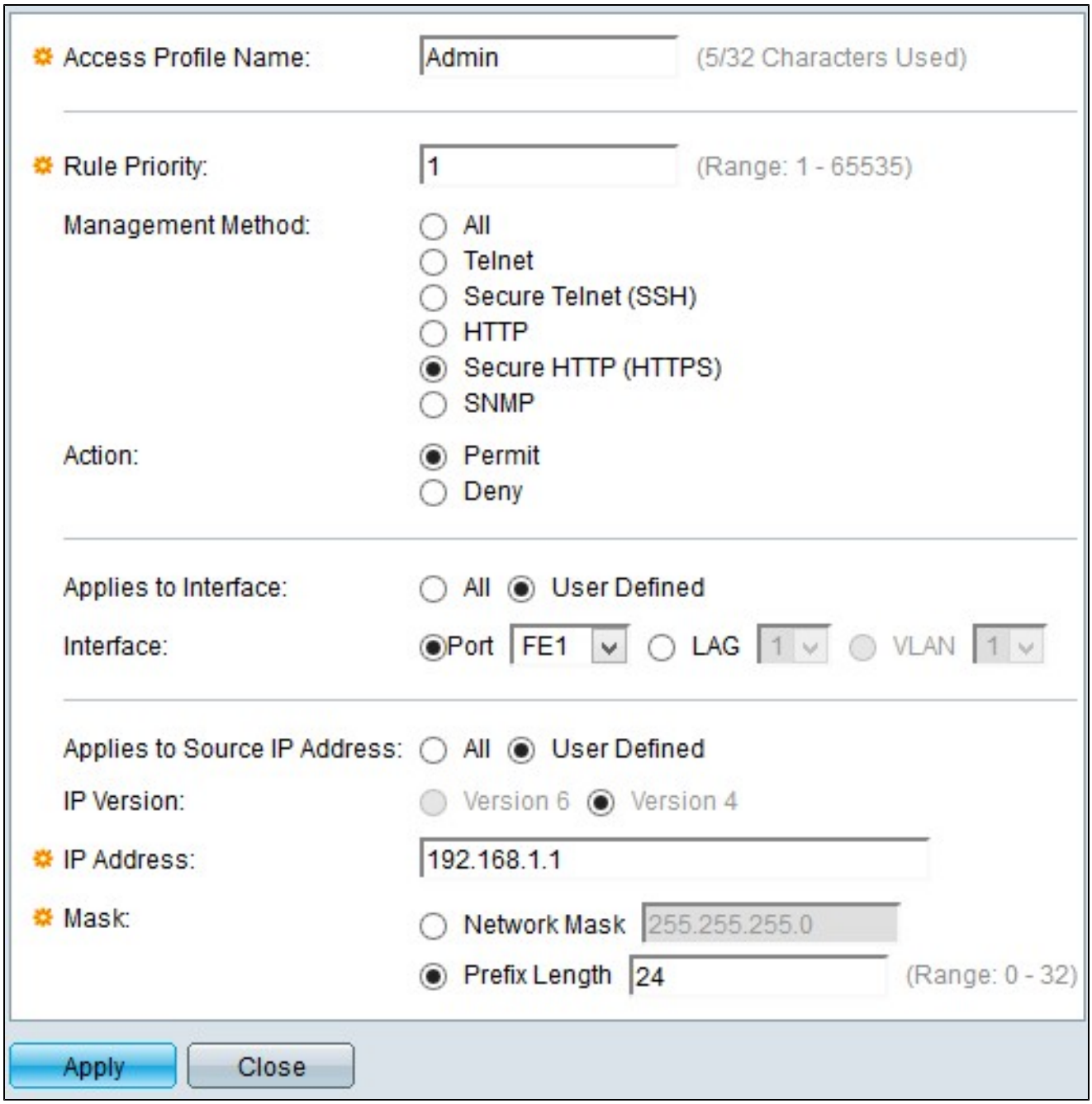
Passaggio 1. Accedere all'utilità di configurazione Web e scegliere Protezione > Metodo di accesso alla gestione > Profili di accesso. Viene visualizzata la pagina Profili di Access:

Passaggio 2. Selezionare il profilo di accesso desiderato dall'elenco a discesa Profilo di accesso attivo.

Passaggio 3. Fare clic su Applica per modificare il profilo di accesso attualmente attivo.

Aggiungi profilo di accesso

Passaggio 1. Fare clic su Aggiungi nella tabella Profilo di accesso. Viene visualizzata la finestra Aggiungi profilo di accesso:



Passaggio 2. Immettere il nome del profilo di accesso nel campo Nome profilo di accesso.

Passaggio 3. Immettere la priorità della regola nel campo Priorità regola. La priorità della regola corrisponde ai pacchetti con le regole. Le regole con priorità inferiore vengono controllate per prime. Se un pacchetto soddisfa una regola, viene eseguita l'azione desiderata.

Passaggio 4. Fare clic sul pulsante di opzione corrispondente al metodo di gestione desiderato nel campo Metodo di gestione. Il metodo di accesso utilizzato dall'utente deve corrispondere al metodo di gestione per l'azione da eseguire. I metodi possibili sono:

· Tutti - Tutti i metodi di gestione vengono assegnati al profilo di accesso.

· Telnet: il metodo di gestione Telnet viene assegnato alla regola. Solo gli utenti con il metodo di accesso alla riunione Telnet dispongono dell'accesso al dispositivo.

· SSH (Secure Telnet): il metodo di gestione SSH è assegnato al profilo. Solo gli utenti con profilo di accesso a riunione Telnet possono accedere al dispositivo.

· HTTP: il metodo di gestione HTTP viene assegnato al profilo. Solo gli utenti con il metodo di profilo di accesso alla riunione HTTP possono accedere al dispositivo.

· HTTP protetto (SSL): il metodo di gestione HTTPS viene assegnato al profilo. Solo gli utenti con il metodo del profilo di accesso alla riunione HTTPS possono accedere al dispositivo.

· SNMP: il metodo di gestione SNMP viene assegnato al profilo. Solo gli utenti con il metodo di accesso alle riunioni SNMP possono accedere al dispositivo.

Passaggio 5. Selezionare l'azione da allegare alla regola dall'elenco a discesa Azione. I valori possibili per l'azione sono:

· Permit (Autorizzazione): l'accesso allo switch è consentito.

· Nega: accesso negato allo switch.

Passaggio 6. Per definire l'interfaccia per il profilo di accesso, fare clic sul pulsante di scelta desiderato corrispondente al tipo di interfaccia desiderato nel campo Si applica a interfaccia. Le due opzioni sono:

· All: include tutte le interfacce, ad esempio porte, VLAN e LAG.

Nota: i LAG sono collegamenti logici che combinano più collegamenti fisici per fornire una maggiore larghezza di banda.

· Definito dall'utente - Si applica solo all'interfaccia desiderata per l'utente.

- Porta: selezionare la porta dall'elenco a discesa Porta per cui si desidera definire il profilo di accesso.

- LAG - Selezionare il LAG dall'elenco a discesa LAG per il quale definire il profilo di accesso dall'elenco a discesa LAG.

- VLAN: selezionare la VLAN dall'elenco a discesa VLAN per cui definire il profilo di accesso dall'elenco a discesa VLAN.

Passaggio 7. Fare clic sul pulsante di opzione Source IP Address (Indirizzo IP di origine) per abilitare l'indirizzo IP di origine dell'interfaccia. Sono disponibili due valori:

· Tutti: include tutti gli indirizzi IP.

· Definito dall'utente: si applica solo all'indirizzo IP desiderato per l'utente.

- Versione 6 — Per indirizzi IP versione 6 (IPv6).

- Versione 4 — Per indirizzi IP versione 4 (IPv4).

Passaggio 8. Se si sceglie Definito dall'utente al punto 7, immettere l'indirizzo IP del dispositivo nel campo Indirizzo IP.

Passaggio 9. Fare clic su un pulsante di scelta nel campo Maschera di una delle opzioni per definire la maschera di rete. Le opzioni disponibili sono:

· Network Mask: consente di immettere la subnet mask che corrisponde all'indirizzo IP nel formato decimale con punti.

· Lunghezza prefisso — immettere la lunghezza del prefisso della subnet mask che corrisponde all'indirizzo IP.

Passaggio 10. Fare clic su Apply (Applica).

Passaggio 11. (Facoltativo) Per eliminare un profilo di accesso, selezionare la casella di controllo del profilo di accesso che si desidera eliminare e fare clic su Elimina.

Passaggio 12. (Facoltativo) Fare clic su Tabella regole profilo per andare alla pagina Regole profilo.

Nota: per ulteriori informazioni sulle regole di profilo, fare riferimento all'articolo Configurazione delle regole di profilo di accesso sugli switch gestiti serie 200/300.

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).