Konfiguration von Zugriffsprofilen auf Managed Switches der Serien 200 und 300

Ziel

Zugriffsprofile fungieren als weitere Sicherheitsebene für den Switch. Zugriffsprofile können aus Sicherheitsgründen bis zu 128 Regeln enthalten. Jede Regel enthält eine Aktion und ein Kriterium. Wenn die Zugriffsmethode nicht mit der Verwaltungsmethode übereinstimmt, wird der Zugriff auf das Gerät für den Benutzer blockiert.

In diesem Artikel wird erläutert, wie Sie Profile für den Zugriff auf die Managed Switches der Serien 200 und 300 konfigurieren.

Unterstützte Geräte

- Managed Switches der Serien SF/SG 200 und SF/SG 300

Software-Version

•1.3.0.62

Konfiguration der Zugriffsprofile

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Mgmt Access Method > Access Profiles**. Die Seite *Access Profiles* (*Zugriffsprofile*) wird geöffnet:

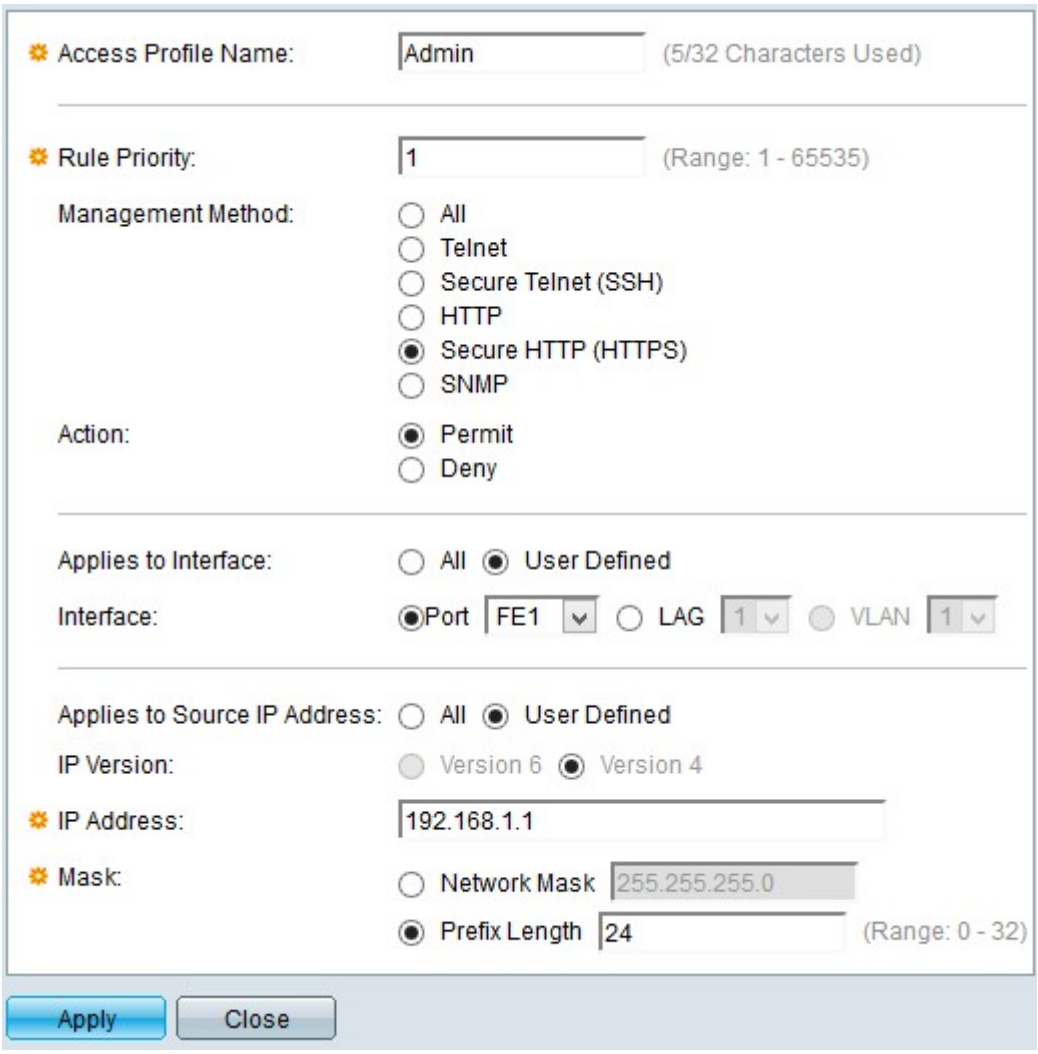
Schritt 2: Wählen Sie das gewünschte Zugriffsprofil aus der Dropdown-Liste Aktives Zugriffsprofil aus.

Schritt 3: Klicken Sie auf **Apply**, um das derzeit aktive Zugriffsprofil zu ändern.

Zugriffsprofil hinzufügen

Schritt 1: Klicken Sie in der Zugriffsprofiltabelle auf **Hinzufügen**. Das Fenster *Add Access*

Profile (Zugriffsprofil hinzufügen) wird angezeigt:



Schritt 2: Geben Sie den Namen des Zugriffsprofils in das Feld "Access Profile Name" (Name des Zugriffsprofils) ein.

Schritt 3: Geben Sie die Priorität der Regel in das Feld "Rule Priority" (Regelpriorität) ein. Die Regelpriorität gleicht Pakete mit Regeln ab. Regeln mit niedrigerer Priorität werden zuerst überprüft. Wenn ein Paket mit einer Regel übereinstimmt, wird die gewünschte Aktion ausgeführt.

Schritt 4: Klicken Sie im Feld Verwaltungsmethode auf das Optionsfeld für die gewünschte Verwaltungsmethode. Die vom Benutzer verwendete Zugriffsmethode muss mit der Verwaltungsmethode für die auszuführende Aktion übereinstimmen. Folgende Methoden sind möglich:

- Alle - Alle Verwaltungsmethoden werden dem Zugriffsprofil zugewiesen.
- Telnet - Die Telnet-Verwaltungsmethode wird der Regel zugewiesen. Nur Benutzer mit Telnet-Meeting-Zugriffsprofilmethode haben Zugriff auf das Gerät.
- Secure Telnet (SSH) - Die SSH-Verwaltungsmethode ist dem Profil zugewiesen. Nur Benutzer mit Telnet-Meeting-Zugriffsprofil haben Zugriff auf das Gerät.
- HTTP — Die HTTP-Verwaltungsmethode ist dem Profil zugewiesen. Nur Benutzer mit HTTP-Meeting-Zugriffsprofilmethode haben Zugriff auf das Gerät.

- Secure HTTP (SSL) - HTTPS-Verwaltungsmethode ist dem Profil zugewiesen. Nur Benutzer mit HTTPS-Meeting-Zugriffsprofilmethode haben Zugriff auf das Gerät.

- SNMP - SNMP-Verwaltungsmethode ist dem Profil zugewiesen. Nur Benutzer mit SNMP-Meeting-Zugriffsprofilmethode haben Zugriff auf das Gerät.

Schritt 5: Wählen Sie aus der Dropdown-Liste Aktion die Aktion aus, die der Regel angefügt werden soll. Mögliche Aktionswerte sind:

- Zulassen - Der Zugriff auf den Switch ist erlaubt.

- Verweigern - Der Zugriff auf den Switch wird verweigert.

Schritt 6: Klicken Sie auf das gewünschte Optionsfeld für den gewünschten Schnittstellentyp im Feld "Schnittstelle anwenden", um die Schnittstelle für das Zugriffsprofil zu definieren. Die beiden Optionen sind:

- Alle - Beinhaltet alle Schnittstellen wie Ports, VLANs und LAGs.

Hinweis: LAGs sind logische Verbindungen, die mehrere physische Verbindungen kombinieren, um mehr Bandbreite bereitzustellen.

- Benutzerdefiniert — Nur auf die gewünschte Benutzeroberfläche für den Benutzer anwenden.

  - Port — Wählen Sie den Port aus der Dropdown-Liste aus, für den das Zugriffsprofil definiert werden soll.

  - LAG: Wählen Sie in der Dropdown-Liste LAG die LAG aus, für die das Zugriffsprofil definiert werden soll.

  - VLAN — Wählen Sie das VLAN aus der VLAN-Dropdown-Liste aus, für das das Zugriffsprofil definiert werden soll.

Schritt 7. Klicken Sie auf das Optionsfeld Quell-IP-Adresse, um die Quell-IP-Adresse der Schnittstelle zu aktivieren. Es gibt zwei mögliche Werte:

- Alle - Beinhaltet alle IP-Adressen.

- Benutzerdefiniert - Nur auf die gewünschte IP-Adresse des Benutzers anwenden.

  - Version 6 - Für IP-Adressen der Version 6 (IPv6).

  - Version 4 - Für IP-Adressen der Version 4 (IPv4).

Schritt 8: Wenn Sie in Schritt 7 die Option Benutzerdefiniert ausgewählt haben, geben Sie die IP-Adresse des Geräts in das Feld IP-Adresse ein.

Schritt 9. Klicken Sie auf ein Optionsfeld im Feld "Mask" (Maske) einer der Optionen, um die Netzwerkmaske zu definieren. Folgende Optionen sind verfügbar:

- Netzwerkmaske — Geben Sie die Subnetzmaske ein, die der IP-Adresse im Dezimalformat mit Punkten entspricht.

- Präfixlänge — Geben Sie die Präfixlänge der Subnetzmaske ein, die der IP-Adresse entspricht.

Schritt 10. Klicken Sie auf **Apply** (Anwenden).

Schritt 11. (Optional) Um ein Zugriffsprofil zu löschen, aktivieren Sie das Kontrollkästchen des Zugriffsprofils, das Sie löschen möchten, und klicken Sie auf **Löschen**.

Schritt 12. (Optional) Klicken Sie auf **Profilregeltabelle**, um die Seite *Profilregeln* aufzurufen.

Hinweis: Weitere Informationen zu Profilregeln finden Sie im Artikel *Access Profile Rules Configuration on 200/300 Series Managed Switches (Konfiguration von Zugriffsprofilregeln für Managed Switches der Serien 200/300)*.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.