Konfigurieren von IPv4-basierten Zugriffslisten auf den Managed Switches der Serien 200 und 300

Ziel

Zugriffslisten sind Regeln, die Sie anwenden können, um einen bestimmten Datenverkehrsfluss in Ihrem Netzwerk zu erlauben oder zu verweigern. Dadurch wird die Sicherheit erhöht und die Gesamtleistung Ihres Netzwerks erhöht.

In diesem Dokument wird erläutert, wie Sie IPv4-basierte Zugriffslisten für die Managed Switches der Serien 200 und 300 konfigurieren.

Unterstützte Geräte

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

Software-Version

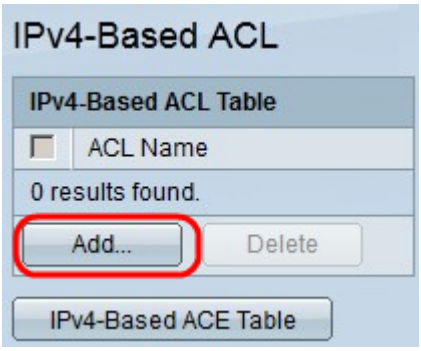
•1.3.0.62

Konfiguration von IPv4-basierter ACL und ACE

IPv4-basierte Zugriffskontrolllisten

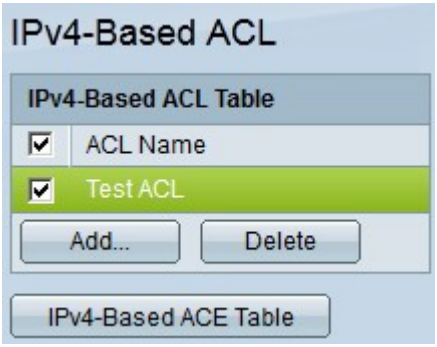
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Access Control > IPv4-Based ACL (Zugriffskontrolle > IPv4-basierte ACL) aus**. Die Seite *IPv4-Based ACL* wird geöffnet.

Schritt 2: Klicken Sie auf **Hinzufügen**, um eine neue Zugriffsliste hinzuzufügen.



Schritt 3: Geben Sie im Feld *ACL Name (ACL-Name)* einen Namen für die neue Zugriffsliste ein.

Schritt 4: Klicken Sie auf **Apply**, um die Zugriffsliste zu speichern.



Schritt 5. (Optional) Um eine Zugriffsliste zu löschen, aktivieren Sie das Kontrollkästchen der Zugriffsliste, die Sie löschen möchten, und klicken Sie auf **Löschen**.

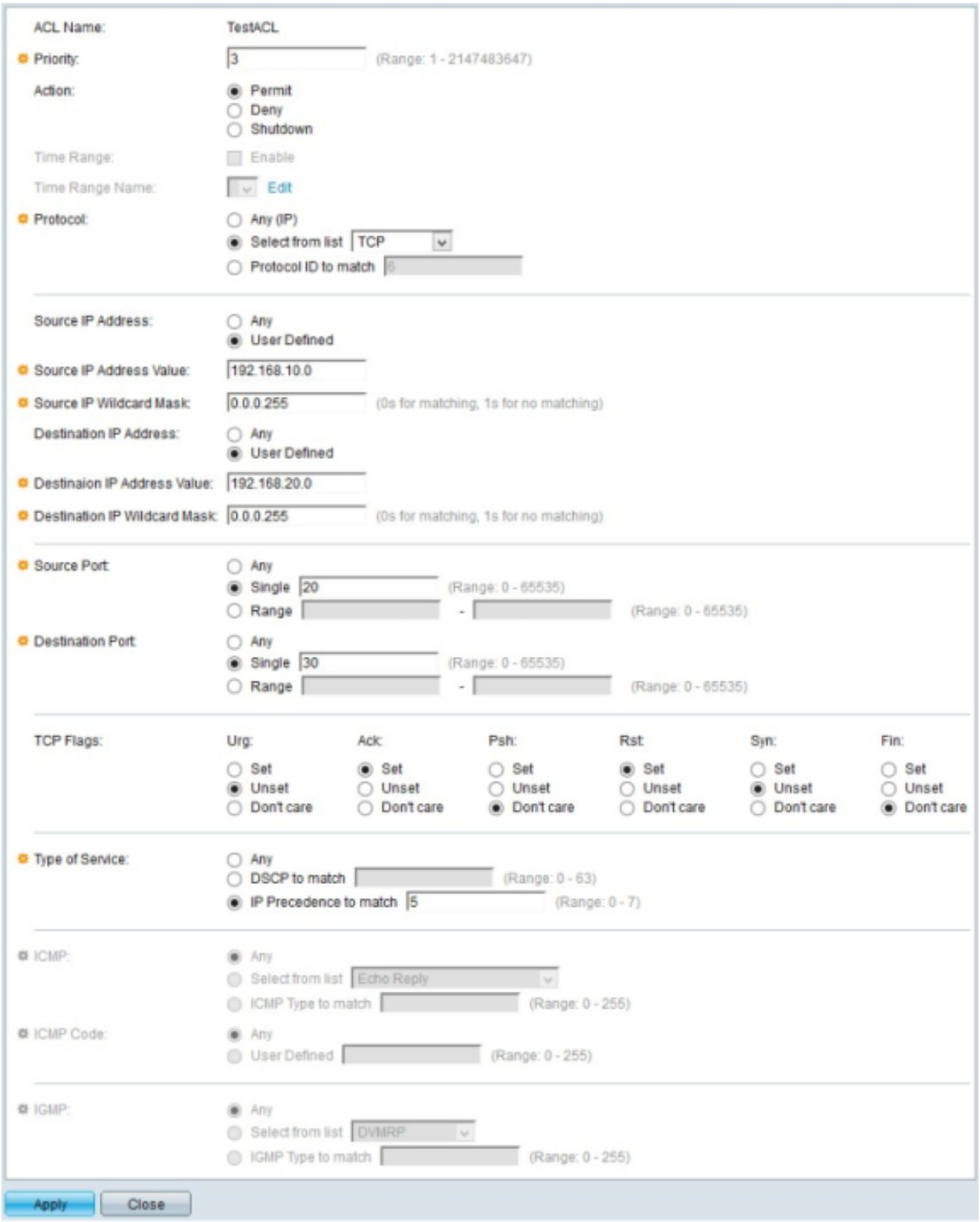
IPv4-basierte ACEs

Um einen ACE mit einer ACL zu verwalten, müssen die nächsten Schritte ausgeführt werden.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Access Control > IPv4-Based ACEs aus**. Die Seite *IPv4-Based ACE* wird geöffnet.

Schritt 2: Wählen Sie in der Dropdown-Liste *Filter: ACL Name (ACL-Name ist gleich*) die Zugriffsliste aus, der Sie eine Zugriffsregel zuweisen möchten.

Schritt 3: Klicken Sie auf **Hinzufügen**. Das Fenster *IP-basierten ACE hinzufügen* wird angezeigt.



Schritt 4: Geben Sie die Priorität des ACE in das Feld *Priority (Priorität*) ein. Der ACE mit der höchsten Priorität wird zuerst verarbeitet. Die höchste Priorität ist 1. Der Bereich liegt zwischen 1 und 2147483647.

Schritt 5: Klicken Sie im Feld *Aktion* auf das Optionsfeld der Aktion, die diese Zugriffsregel ausführen soll. Folgende Optionen sind verfügbar:

- Zulassen - Leitet Pakete gefiltert vom aktuellen ACE weiter.

- Verweigern - Verwirft Pakete, die vom aktuellen ACE gefiltert werden.

- Herunterfahren - Verwirft Pakete, die vom aktuellen ACE gefiltert werden, und deaktiviert den Port, von dem die Pakete empfangen wurden.

Schritt 6: Klicken Sie im Feld *Protocol* (Protokoll) auf das Optionsfeld des Protokolls, das Sie dem ACE hinzufügen möchten. Der ACE wird für alle gerouteten Netzwerkprotokolle konfiguriert, um die Pakete beim Durchlaufen eines Routers zu filtern. Folgende Optionen sind verfügbar:

- Beliebig: Wählt eines der IPv4-basierten ACE-Protokolle.

- Wählen Sie aus der Liste — Wählen Sie das gewünschte Protokoll aus der Dropdown-Liste aus.

- Übereinstimmende Protokoll-ID — Mit dieser Option können Sie die Protokoll-ID eingeben, die Sie verwenden möchten.

Schritt 7. Klicken Sie im Feld *Quell-IP-Adresse* auf eine der verfügbaren Optionen als Quell-IP-Adresse:

- Beliebig - Diese Option wendet die Zugriffsregel auf alle IP-Adressen an, die in einem bestimmten Netzwerksegment verfügbar sind.

- Benutzerdefiniert - Mit dieser Option können Sie eine bestimmte IP-Adresse eingeben.

  - Quell-IP-Adresswert — Geben Sie in dieses Feld die Quell-IP-Adresse ein.

  - Source IP Wildcard Mask (Quell-IP-Platzhaltermaske) - Geben Sie in diesem Feld die Platzhaltermaske der Quell-IP-Adresse ein. Mit der Platzhaltermaske können Sie angeben, auf welchen Host der Quell-IP-Adresse diese Zugriffsliste angewendet wird.

Schritt 8: Klicken Sie im Feld *Ziel-IP-Adresse* auf eine der verfügbaren Optionen als Ziel-IP-Adresse:

- Beliebig - Diese Option wendet die Zugriffsregel auf alle IP-Adressen an, die in einem bestimmten Netzwerksegment verfügbar sind.

- Benutzerdefiniert - Mit dieser Option können Sie eine bestimmte IP-Adresse eingeben, um die Zugriffsregel anzuwenden:

  - Wert der Ziel-IP-Adresse — Geben Sie in dieses Feld die Ziel-IP-Adresse ein.

  - Ziel-IP-Wildcard-Maske — Geben Sie in diesem Feld die Wildcard-Maske der Ziel-IP-Adresse ein. Mit der Platzhaltermaske können Sie angeben, auf welche Hosts der Ziel-IP-Adresse diese Zugriffsliste angewendet wird.

Schritt 9. Das Feld *Quellport* ist nur aktiviert, wenn Sie in Schritt 5 TCP oder UDP auswählen. Klicken Sie auf das Optionsfeld einer der verfügbaren Optionen, um den Quellport auszuwählen:

- Beliebig - Diese Option akzeptiert alle Quellports.

- Einfach - Mit dieser Option können Sie einen einzelnen Quell-Port-Wert eingeben.

- Bereich - Mit dieser Option können Sie einen Bereich verfügbarer Quell-Ports eingeben.

Schritt 10. Das Feld *Zielport* ist nur aktiviert, wenn Sie in Schritt 5 TCP oder UDP auswählen. Klicken Sie auf das Optionsfeld einer der verfügbaren Optionen, um den Zielport auszuwählen:

- Beliebig - Diese Option akzeptiert alle Zielports.
- Single - Mit dieser Option können Sie einen einzigen Zielport-Wert eingeben.
- Bereich - Mit dieser Option können Sie einen Bereich verfügbarer Ziel-Ports eingeben.

Schritt 11. Das Feld *TCP-Flags* ist nur aktiviert, wenn Sie TCP aus Schritt 5 auswählen. Klicken Sie auf eines der Optionsfelder für jedes Flag, um den gewünschten Status für die Zugriffsregel auszuwählen:

- Urg — Diese Markierung identifiziert eingehende Daten als dringend.
- Ack (Bestätigen): Diese Markierung wird verwendet, um den Empfang von Paketen zu bestätigen.
- Psh - Diese Markierung wird verwendet, um sicherzustellen, dass die Daten die richtige Priorität erhalten und auf der Sende- oder Empfangsseite verarbeitet werden.
- Rst - Dieses Flag wird verwendet, wenn eine Verbindung ein falsches Segment empfängt.
- Syn - Dieses Flag wird für TCP-Kommunikation verwendet.
- Finn - Dieses Flag wird verwendet, wenn die Kommunikation oder Datenübertragung beendet ist.

Schritt 12: Klicken Sie im Feld *Type of Service (Servicetyp*) auf eines der verfügbaren Optionsfelder, um einen Servicetyp für das IP-Paket auszuwählen:

- Beliebig - Diese Option wählt jede Art von Service.
- Übereinstimmender DSCP - Wählen Sie diese Option, um DSCP (Differentiated Service Code Point) als einen Servicetyp zu implementieren. DSCP ist ein Mechanismus zur Klassifizierung und Verwaltung des Netzwerkverkehrs. Geben Sie den DSCP-Wert ein, den Sie auf die Zugriffsregel anwenden möchten.
- Abzugleichende IP-Rangfolge - Dieser Servicetyp wird vom aktuellen Netzwerk verwendet, um die richtige QoS (Quality of Service) bereitzustellen. Geben Sie den Wert ein, den Sie auf die Zugriffsregel anwenden möchten.

Schritt 13: Das Feld *"ICMP (Internet Control Message Protocol)*" ist nur aktiviert, wenn Sie in Schritt 5 "ICMP" auswählen. ICMP wird verwendet, um Fehlermeldungen zu senden, wenn ein Dienst nicht verfügbar ist, oder um die Verbindung zu testen. Klicken Sie auf eines der verfügbaren Optionsfelder, um die ICMP-Nachrichtentypen zu filtern:

- Beliebig - Es kann sich um eine der Fehlermeldungen oder Abfragemeldungen handeln.
- Wählen Sie eine der zulässigen Kontrollmeldungen aus der Dropdown-Liste aus.
- Abzugleichender ICMP-Typ — Mit dieser Option können Sie die Anzahl der ICMP-Typen

eingeben, die Sie filtern möchten.

Schritt 14: Das Feld *ICMP-Code* ist nur aktiviert, wenn Sie in Schritt 5 ICMP auswählen. ICMP-Codes werden verwendet, um spezifischere Informationen über die Kontrollnachrichten bereitzustellen. Klicken Sie auf eine der verfügbaren Optionen:

- Beliebig - Es kann sich um einen beliebigen Wert handeln, der mit der Kontrollnachricht übereinstimmt.
- Benutzerdefiniert — Geben Sie den ICMP-Code ein, den Sie filtern möchten.

Schritt 15: Das Feld *IGMP (Internet Group Management Protocol*) ist nur aktiviert, wenn Sie IGMP aus Schritt 5 auswählen. IGMP verwaltet die Hostmitgliedschaft in IP-Multicast-Gruppen in einem Netzwerksegment. Klicken Sie auf eines der verfügbaren Optionsfelder, um IGMP-Nachrichtentypen zu filtern:

- Beliebig - Diese Option akzeptiert alle IGMP-Nachrichtentypen.

- Wählen Sie aus der Liste — Wählen Sie eine der verfügbaren Optionen aus der Dropdown-Liste aus, um zu filtern:

- DVMRP - Verwendet ein Reverse Path Flooding-Verfahren, bei dem eine Kopie eines empfangenen Pakets über jede Schnittstelle mit Ausnahme der Schnittstelle gesendet wird, an der das Paket angekommen ist.

- Host-Abfrage - Es sendet regelmäßig allgemeine Host-Abfragemeldungen zu jedem angeschlossenen Netzwerk, um Informationen zu erhalten.

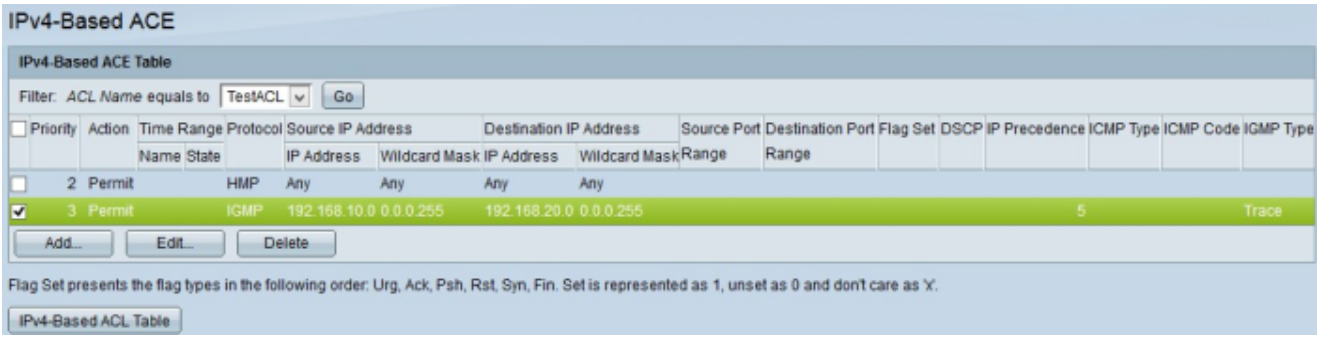
- Host-Reply — Es antwortet auf die Anfrage .

- PIM: Wird zwischen dem lokalen und dem Remote-Multicast-Router verwendet, um Multicast-Datenverkehr vom Multicast-Server an eine Vielzahl von Multicast-Clients weiterzuleiten.

- Trace - Stellt Informationen zum Beitreten und Verlassen einer IGMP-Multicast-Gruppe bereit.

- IGMP-Übereinstimmungstyp — Mit dieser Option können Sie die Anzahl der IGMP-Typen eingeben, die Sie filtern möchten.

Schritt 16: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.



Schritt 17. (Optional) Um eine aktuelle Zugriffsregel zu bearbeiten, aktivieren Sie das Kontrollkästchen der Zugriffsregel, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

Schritt 18. (Optional) Um eine aktuelle Zugriffsregel zu löschen, aktivieren Sie das Kontrollkästchen der Zugriffsregel, die Sie löschen möchten, und klicken Sie auf **Löschen**.

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.