IPv4-gebaseerde toegangslijsten op de 200/300 Series beheerde Switches configureren

Doel

Toegangslijsten zijn regels die u kunt toepassen om specifieke verkeersstromen op uw netwerk toe te staan of te ontkennen, wat meer beveiliging toevoegt en de algemene prestaties op uw netwerk verhoogt.

Het doel van dit document is u te tonen hoe u op IPv4 gebaseerde toegangslijsten op de 200/300 Series beheerde Switches kunt configureren.

Toepasselijke apparaten

· SF/SG 200 en SF/SG 300 Series beheerde Switches

Softwareversie

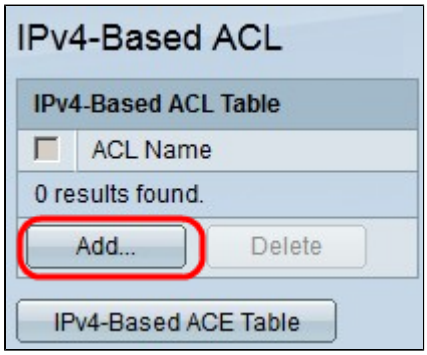
â€¢1.3.0.62

Configuratie van IPv4-gebaseerde ACL en ACE

IPv4-gebaseerde ACLâ€™s

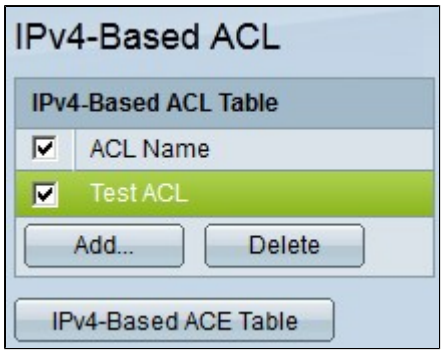
Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Toegangsbeheer > op IPv4 gebaseerde ACL**. De *op IPv4 gebaseerde ACL*-pagina wordt geopend.

Stap 2. Klik op **Add** om een nieuwe toegangslijst toe te voegen.



Stap 3. Voer in het veld *ACL-naam* een naam in voor de nieuwe toegangslijst.

Stap 4. Klik op **Toepassen** om de toegangslijst op te slaan.

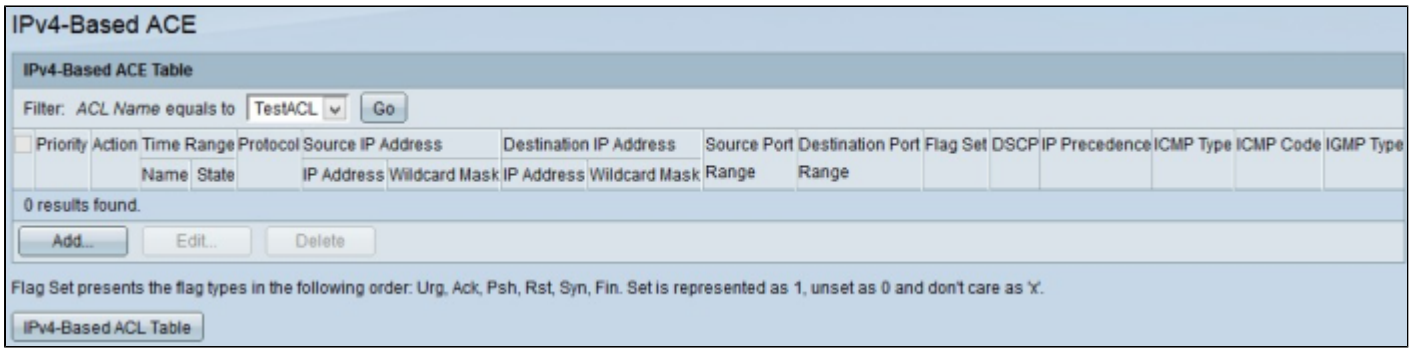


Stap 5. (Optioneel) Als u een toegangslijst wilt verwijderen, schakelt u het aanvinkvakje van de toegangslijst in en klikt u op **Verwijderen**.

IPv4-gebaseerde ACEâ€™s

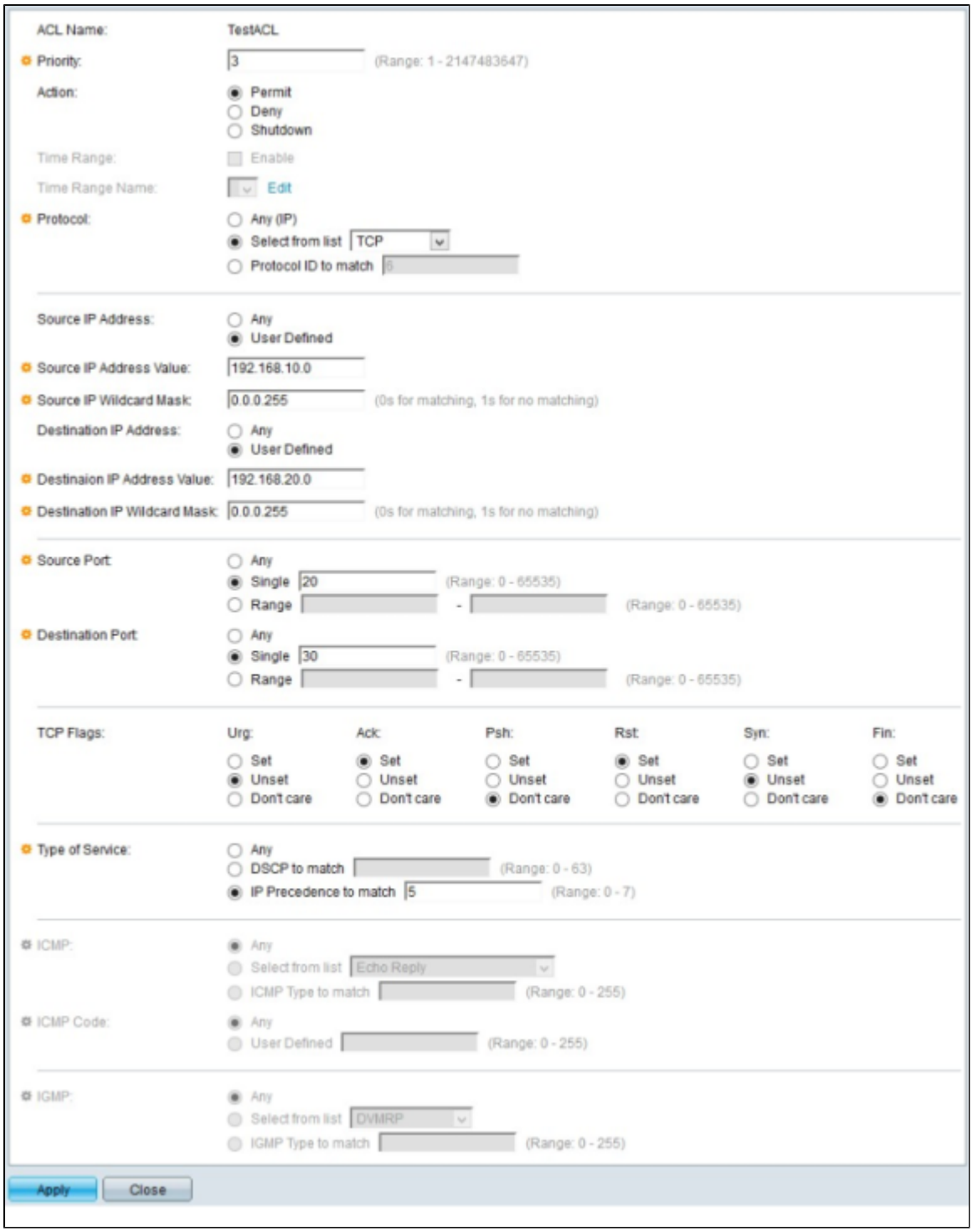
Om een ACE aan ACL te beheren, moeten de volgende stappen worden gevolgd.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Toegangsbeheer > op IPv4 gebaseerde ACEâ€™s**. De *op IPv4 gebaseerde ACE*-pagina wordt geopend.



Stap 2. In het *filter: ACL-naam is gelijk aan* vervolgkeuzelijst. Kies de toegangslijst die u wilt toewijzen aan een toegangsregel.

Stap 3. Klik op **Add** (Toevoegen). Het *Add IP-gebaseerde ACE*-venster verschijnt.



Stap 4. Voer in het veld *Prioriteit* de prioriteit van ACE in. De ACE met de hoogste prioriteit wordt eerst verwerkt. De hoogste prioriteit is 1. Het heeft een bereik van 1 tot 2147483647.

Stap 5. Klik in het veld *Actie* op het keuzerondje van de actie die u met deze toegangsregel wilt uitvoeren. De beschikbare opties zijn:

· Vergunning â€" voorwaartse pakketten die door huidige ACE worden gefiltreerd.

· Deny â€" Drops pakketten die worden gefilterd door de huidige ACE.

· Uitschakelen â€" Dropt pakketten die worden gefilterd door de huidige ACE en schakelt de poort uit waar de pakketten werden ontvangen.

Stap 6. Klik in het veld *Protocol* op de radioknop van het protocol dat u in ACE wilt toevoegen. ACE wordt gevormd voor alle gerouteerde netwerkprotocollen om de pakketten te filteren aangezien de pakketten door een router overgaan. De beschikbare opties zijn:

· Alle â€" kiest een van de op IPv4 gebaseerde ACE-protocollen.

· Selecteer uit lijst â€" Kies het gewenste protocol uit de vervolgkeuzelijst.

· Protocol-ID te matchen â€" Met deze optie kunt u de protocol-ID invoeren die u wilt gebruiken.

Stap 7. Klik in het veld *IP-bronadres* op een van de beschikbare opties als IP-bronadres:

· Om het even welk â€" Deze optie past de toegangsregel op om het even welke IP adressen toe beschikbaar in een specifiek netwerksegment.

· Door gebruiker gedefinieerd â€" met deze optie kunt u een specifiek IP-adres invoeren.

- IP-bronadreswaarde â€" Voer in dit veld het IP-bronadres in.

- IP-bronjokermasker â€" Voer in dit veld het jokermasker van het IP-bronadres in. Met het wildkaartmasker kunt u specificeren op welke host van het IP-bronadres deze toegangslijst wordt toegepast.

Stap 8. Klik in het veld *IP-adres bestemming* op een van de beschikbare opties als IP-adres voor bestemming:

· Om het even welk â€" Deze optie past de toegangsregel op om het even welke IP adressen toe beschikbaar in een specifiek netwerksegment.

· Door gebruiker gedefinieerd â€" met deze optie kunt u een specifiek IP-adres invoeren om de toegangsregel toe te passen:

- Waarde IP-adres van bestemming â€" Voer in dit veld het IP-adres van bestemming in.

- IP-jokermasker van bestemming â€" Voer in dit veld het jokermasker van het IP-adres van bestemming in. Met het wildkaartmasker kunt u specificeren op welke hosts van het IP-adres van de bestemming deze toegangslijst wordt toegepast.

Stap 9. Het veld *Source Port* is alleen ingeschakeld wanneer u TCP of UDP in Stap 5 kiest. Klik op het keuzerondje van een van de beschikbare opties om de bronpoort te kiezen:

· Om het even welk â€" Deze optie keurt om het even welke bronhaven goed.

· Enkelvoudig â€" met deze optie kunt u één poortwaarde voor één bron invoeren.

· Bereik â€" Met deze optie kunt u een reeks beschikbare bronpoorten invoeren.

Stap 10. Het veld *Doelpoort* is alleen ingeschakeld wanneer u TCP of UDP in Stap 5 kiest. Klik op het keuzerondje van een van de beschikbare opties om de bestemmingshaven te kiezen:

· Om het even welk â€" Deze optie keurt om het even welke bestemmingshaven goed.

· Enkelvoudig â€" Met deze optie kunt u één poortwaarde voor één bestemming invoeren.

· Bereik â€" Met deze optie kunt u een reeks beschikbare bestemmingspoorten invoeren.

Stap 11. Het veld *TCP-vlaggen* wordt alleen ingeschakeld als u TCP kiest uit Stap 5. Klik op een van de radioknoppen voor elke vlag om te kiezen welke staat u de toegangsregel wilt activeren:

· Urg â€” Deze markering identificeert inkomende gegevens als urgent.

· Ack â€” Deze vlag wordt gebruikt om de ontvangst van pakketten met succes te bevestigen.

· Psh â€” Deze markering wordt gebruikt om ervoor te zorgen dat de gegevens de juiste prioriteit krijgen en worden verwerkt aan de verzendende of ontvangende kant.

· Rst â€” Deze vlag wordt gebruikt wanneer een verbinding een verkeerd segment ontvangt.

· Syn â€” Deze vlag wordt gebruikt voor TCP-communicatie.

· Fin â€” Deze markering wordt gebruikt wanneer de communicatie of gegevensoverdracht is voltooid.

Stap 12. Klik in het veld *Type of Service* op een van de beschikbare radioknoppen om een type service voor het IP-pakket te kiezen:

· Om het even welk â€” Deze optie kiest om het even welk type van dienst.

· DSCP bij overeenkomst â€” Kies deze optie om een gedifferentieerd servicecode (DSCP) te implementeren als een type service. DSCP is een mechanisme om netwerkverkeer te classificeren en te beheren. Voer de DSCP-waarde in die u op de toegangsregel wilt toepassen.

· Te matchen IP-voorrang â€” Dit type service wordt door het huidige netwerk gebruikt om de juiste QoS (Quality of Service) te bieden. Voer de waarde in die u op de toegangsregel wilt toepassen.

Stap 13. Het veld *ICMP (Internet Control Message Protocol)* wordt alleen ingeschakeld wanneer u ICMP in stap 5 kiest. ICMP wordt gebruikt om foutmeldingen te verzenden wanneer een service niet beschikbaar is of om de verbinding te testen. Klik op een van de beschikbare radioknoppen om ICMP-berichttypen te filteren:

· Om het even welk â€" Het kan om het even welke foutenmeldingen of vraagberichten zijn.

· Selecteer uit lijst â€" Kies een van de toegestane besturingsberichten uit de vervolgkeuzelijst.

· ICMP-type om aan te passen â€" met deze optie kunt u het aantal ICMP-typen invoeren dat u wilt filteren.

Stap 14. Het veld *ICMP-code* wordt alleen ingeschakeld wanneer u ICMP kiest uit Stap 5. De codes ICMP worden gebruikt om specifiekere informatie over de controleberichten te verstrekken. Klik op

een van de beschikbare opties:

· Om het even welk â€" Het kan om het even welke waarde zijn die het controlebericht aanpast.

· Door gebruiker gedefinieerd â€" Voer de ICMP-code in die u wilt filteren.

Stap 15. Het veld *IGMP (Internet Group Management Protocol)* wordt alleen ingeschakeld wanneer u IGMP kiest uit Stap 5. IGMP beheert hostlidmaatschap in IP-multicast groepen op een netwerksegment. Klik op een van de beschikbare radioknoppen om IGMP-berichttypen te filteren:

· Om het even welk - Deze opties keurt alle IGMP berichttypes goed.

· Selecteer uit lijst â€" Kies een van de beschikbare opties in de vervolgkeuzelijst om te filteren:

- DVMRP - het gebruikt een omgekeerde weg overstromende techniek, die een exemplaar van een ontvangen pakket door elke interface behalve waaruit het pakket aankwam verstuurt.

- Host-Query â€" Het stuurt periodiek algemene host-query-berichten op elk aangesloten netwerk voor informatie

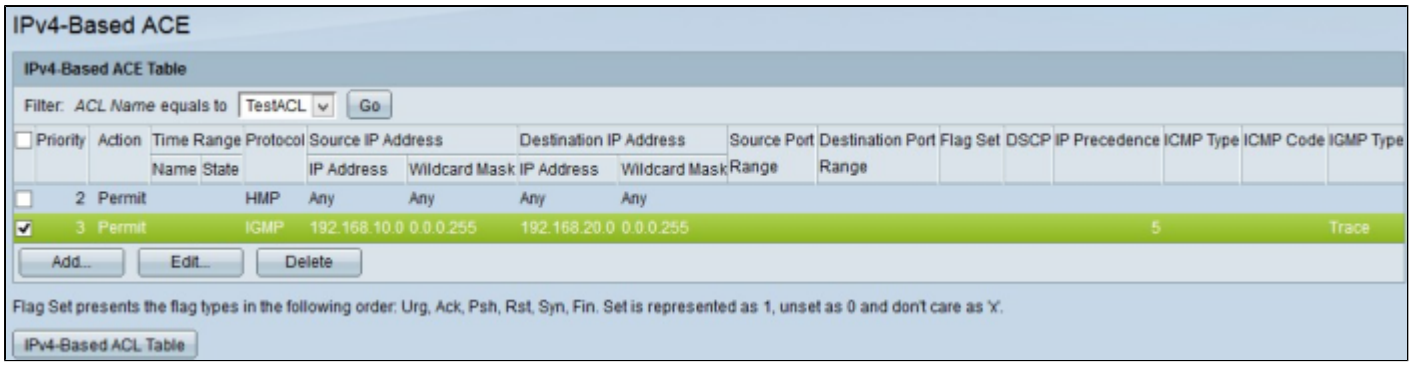
- Host-Reply (host-antwoord) â€" Antwoorden op de vraag .

- PIM â€" Het wordt gebruikt tussen de lokale en externe multicast routers om multicast verkeer van de multicast server naar vele multicast clients te leiden.

- Trace - het geeft informatie om een IGMP multicast groep aan te sluiten en te verlaten.

· IGMP-type overeenkomst â€" Met deze optie kunt u het aantal IGMP-typen invoeren dat u wilt filteren.

Stap 16. Klik op **Toepassen** om de configuratie op te slaan.



Stap 17. (Optioneel) Als u een huidige toegangsregel wilt bewerken, schakelt u het aankruisvakje in van de toegangsregel die u wilt bewerken en klikt u op **Bewerken**.

Stap 18. (Optioneel) Als u een huidige toegangsregel wilt verwijderen, schakelt u het aanvinkvakje van de toegangsregel die u wilt verwijderen in en klikt u op **Verwijderen**.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.