

Overzicht van downloadbare ACL in Catalyst 1300 Switches

Doel

Het doel van dit artikel is om u een overzicht te bieden van de downloadbare ACL (DACL) -functie in Catalyst 1300-switches.

Toepasselijke apparaten | Softwareversie

- Katalysator 1300-serie | 4.1.6.54

Inleiding

ACL's zijn ACL's die aan een switch-poort zijn toegewezen op basis van een beleid of criteria zoals gebruikersaccountgroep, lidmaatschap, tijdstip van de dag en meer. Dit kunnen lokale ACL's zijn die zijn opgegeven door filter-ID of downloadbare ACL's (DACL).

Downloadbare ACL's zijn dynamische ACL's die worden gemaakt en gedownload van de Cisco ISE-server. Ze passen dynamisch toegangscontroleregels toe op basis van gebruikersidentiteit en apparaattype. DACL heeft het voordeel dat u één centrale repository voor ACL's kunt hebben, dus u hoeft ze niet handmatig op elke switch te maken. Wanneer een gebruiker verbinding maakt met een switch, hoeft deze alleen maar te worden geverifieerd en de switch downloadt de toepasselijke ACL's van de Cisco ISE-server.

Inhoud

- [Overwegingen voor DACL](#)
- [DACL-downloadproces](#)
- [Downloadbare ACL-namen](#)

Overwegingen voor DACL

Er zijn een paar dingen om in gedachten te houden bij het werken met DACL op Catalyst 1300-switches.

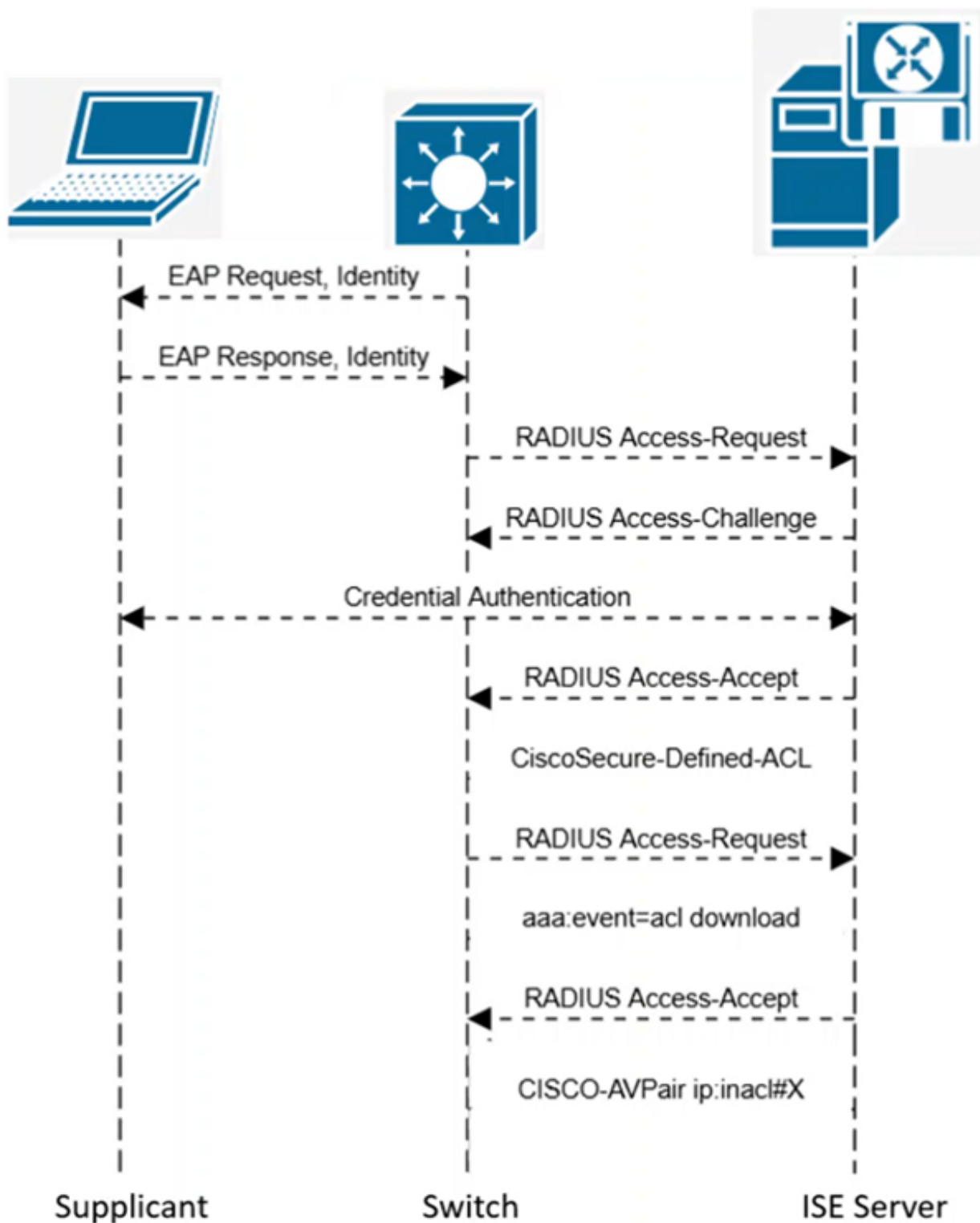
- Deze functie is exclusief voor de Catalyst 1300-switches; het wordt niet ondersteund op de

Catalyst 1200-switches.

- Dynamische ACL's worden niet ondersteund op interfaces waarop een beleidskaart is toegepast.
 - Switch zal geen toegangsverzoek voor ACL-regels verzenden.
 - De aanvrager wordt ingesteld op Geverifieerde maar niet geautoriseerde staat.
- Dynamische ACL's sluiten elkaar wederzijds uit met IP Source Guard en (interface niveau) security-suite gerelateerde configuratie
- Bij het gebruik van dynamische ACL's met gestapelde switches zijn er enkele punten om te overwegen.
 - Als de Active-eenheid uitvalt, worden de DACL's niet opgeslagen in het lokale switch van de nieuwe Active-eenheid en moeten alle DACL's opnieuw worden gedownload.
 - Alle regels die zijn toegepast op interfaces die zijn toegewezen als onderdeel van de verificatie van het clientsysteem, worden verwijderd.
- Het is noodzakelijk om MAC-verificatietype in te stellen op RADIUS (in plaats van de standaard EAP-methode) als u MAB (MAC Authentication Bypass) gebruikt.
- ACL-naamlengte
 - DACL: 64 tekens
 - Statisch: 32 tekens
- Dynamische ACL's zijn allemaal uitgebreide ACL's.
- DACL's gebruiken meer TCAM-bronnen dan u zou verwachten.
- Downloadbare ACL's worden automatisch verwijderd als er geen poorten zijn die deze ACL gebruiken.
- De standaard-ACL die is gemaakt voor dynamische ACL's wordt automatisch verwijderd als er geen poorten zijn die dynamische of downloadbare ACL's gebruiken.

DACL-downloadproces

- Begint als een standaard 802.1x-verificatie.
- Nadat de client is geverifieerd
 - ISE-server verzendt RADIUS Access-Accept met Cisco Vendor AVPair – ACS: CiscoSecure-Defined-ACL = <ACL Name>
 - Switch verzendt RADIUS Access-Request met Cisco Vendor AVPair – aaa: event=acl-download
 - ISE-server verzendt RADIUS Access-Accept met Cisco-leverancier AVPair-ip: inacl#<Aantal ACE-vermeldingen> = ACE



Downloadbare ACL-namen

De naam die wordt gedownload en toegewezen aan de DACL op de switch is niet hetzelfde als de DACL die u maakt op ISE.

Als er bijvoorbeeld een DACL met de naam Marketing_ACL wordt gemaakt in ISE, kan

deze bij het downloaden verschijnen als #ACSACL#-IP-Marketing_ACL-57f6b0d4.

- Formaat op ISE-server: <naam> - ex: Marketing_ACL
- Formaat gedownload naar C1300 Switch
 - #ACSACL#-IP-<name>-<number>
 - ex: #ACSACL#-IP-Marketing_ACL-57f6b0d4
- Naam segmenten
 - #ACSACL# - Prefix toegevoegd door ISE
 - IP – geeft het type ACL (IP ACL) aan
 - <name> - Naam van de ACL gemaakt op ISE
 - <number> - versienummer in ASCII-hex
- De lengte van de naam mag niet meer dan 64 tekens bedragen
- Ingekapseld in Cisco-AVPair: ACS:CiscoSecure-Defined-ACL= <Naam gedownload>

Conclusie

Nu u alles weet over downloadbare ACL in Catalyst 1300 switch, bekijk het artikel [Downloadbare ACL in Catalyst 1300 Switches](#) voor stappen om het te configureren.

Raadpleeg de [Catalyst 1300-beheerdershandleiding](#) en de [ondersteuningspagina](#) van de [Cisco Catalyst 1300-reeks voor](#) meer informatie.

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.