Übersicht über herunterladbare ACLs für Catalyst Switches der Serie 1300

Ziel

Ziel dieses Artikels ist es, Ihnen einen Überblick über die herunterladbaren ACL-Funktionen (DACL) der Catalyst 1300-Switches zu geben.

Unterstützte Geräte | Software-Version

- Catalyst 1300-Serie | 4.1.6.54

Einleitung

Dynamische ACLs sind ACLs, die einem Switch-Port anhand einer Richtlinie oder bestimmter Kriterien (z. B. Mitgliedschaft in einer Benutzergruppe, Tageszeit usw.) zugewiesen werden. Dabei kann es sich um lokale ACLs handeln, die durch die Filter-ID oder durch herunterladbare ACLs (DACLs) angegeben werden.

Herunterladbare ACLs sind dynamische ACLs, die vom Cisco ISE-Server erstellt und heruntergeladen werden. Sie wenden Zugriffskontrollregeln basierend auf der Benutzeridentität und dem Gerätetyp dynamisch an. DACL bietet den Vorteil, dass Sie über ein zentrales Repository für ACLs verfügen, sodass Sie diese nicht auf jedem Switch manuell erstellen müssen. Wenn ein Benutzer eine Verbindung zu einem Switch herstellt, muss er sich lediglich authentifizieren, und der Switch lädt die entsprechenden ACLs vom Cisco ISE-Server herunter.

Inhalt

- DACL-Überlegungen
- DACL-Downloadprozess
- Herunterladbare ACL-Namen

DACL-Überlegungen

Bei der Verwendung von DACL auf Catalyst 1300-Switches müssen einige Punkte berücksichtigt werden.

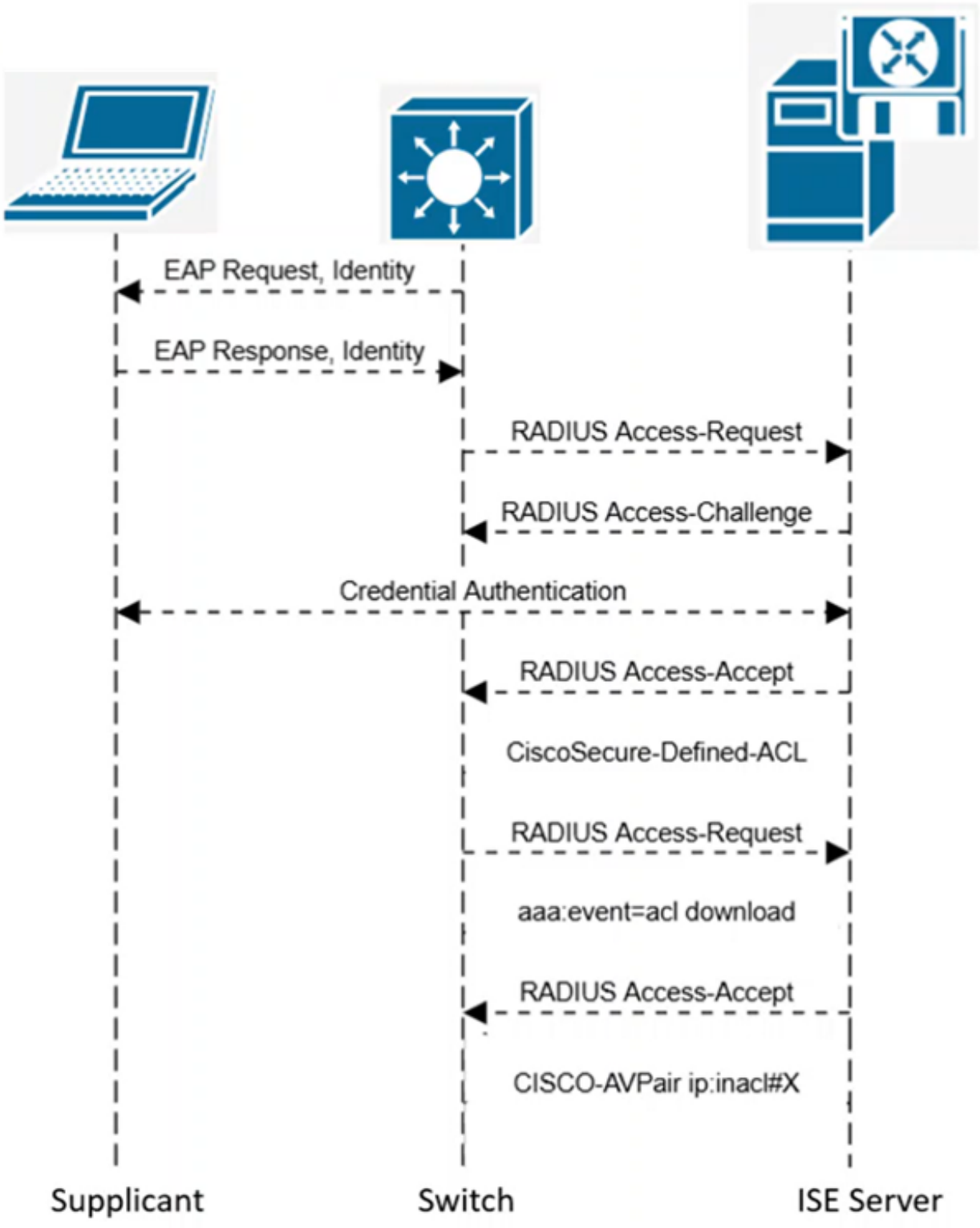
- Diese Funktion steht nur bei Catalyst Switches der Serie 1300 zur Verfügung. wird von den

Catalyst 1200 Switches nicht unterstützt.

- Dynamische ACLs werden auf Schnittstellen mit angewendeter Richtlinienzuordnung nicht unterstützt.
    - Der Switch sendet keine Zugriffsanfragen für ACL-Regeln.
    - Supplicant wird auf den Authentifizierungs-, jedoch nicht auf den Autorisierungs-Status gesetzt.
- Dynamische ACLs schließen sich mit IP Source Guard und der Konfiguration (auf Schnittstellenebene) der Security Suite gegenseitig aus.
- Bei der Verwendung von dynamischen ACLs mit Stack-Switches sind einige Punkte zu beachten.
    - Bei einem Failover des aktiven Geräts werden die DACLs auf dem neuen aktiven Switch nicht im lokalen Speicher gespeichert, und alle DACLs müssen neu heruntergeladen werden.
    - Alle Regeln, die auf Schnittstellen angewendet werden, die im Rahmen der Authentifizierung des Client-Systems zugewiesen wurden, werden entfernt.
- Wenn Sie MAB (MAC Authentication Bypass) verwenden, müssen Sie den MAC Authentication Type auf RADIUS (statt auf die Standard-EAP-Methode) festlegen.
- Länge des ACL-Namens
    - DACL: 64 Zeichen
    - Statisch: 32 Zeichen
- Dynamische ACLs sind erweiterte ACLs.
- DACLs verwenden mehr TCAM-Ressourcen, als Sie vielleicht erwarten.
- Herunterladbare ACLs werden automatisch gelöscht, wenn keine Ports diese ACL verwenden.
- Die für dynamische Zugriffskontrolllisten erstellte Standard-Zugriffskontrollliste wird automatisch gelöscht, wenn keine Ports dynamische oder herunterladbare Zugriffskontrolllisten verwenden.

DACL-Downloadprozess

- Startet als Standard-802.1x-Authentifizierung.
- Nach der Client-Authentifizierung
    - ISE-Server sendet RADIUS Access-Accept mit Cisco Vendor AVPair - ACS:CiscoSecure-Defined-ACL = <ACL-Name>
    - Switch sendet RADIUS-Zugriffsanfrage mit Cisco Vendor AVPair - aaa:event=acl-download
    - ISE-Server sendet RADIUS Access-Accept mit Cisco Vendor AVPair-ip:inacl#<Nummer des ACE-Eintrags> = ACE



Herunterladbare ACL-Namen

Der Name, der heruntergeladen und der DACL auf dem Switch zugewiesen wird, ist nicht der gleiche wie der DACL, den Sie auf der ISE erstellen.

Wenn beispielsweise eine DACL mit dem Namen Marketing_ACL in der ISE erstellt

wird, kann sie beim Herunterladen als #ACSACL#-IP-Marketing_ACL-57f6b0d4 angezeigt werden.

- Format auf ISE-Server: <Name> - Beispiel: Marketing_ACL
- Auf C1300-Switch heruntergeladenes Format
    - #ACSACL#-IP-<Name>-<Nummer>
    - Beispiel: #ACSACL#-IP-Marketing_ACL-57f6b0d4
- Namenssegmente
    - #ACSACL# - Präfix von ISE hinzugefügt
    - IP: Gibt den Typ der ACL an (IP ACL).
    - <Name> - Name der auf der ISE erstellten ACL
    - <Nummer> - Versionsnummer in ASCII-Hex
- Die Namenslänge muss kleiner oder gleich 64 Zeichen sein.
- Kapselt in Cisco-AVPair: ACS:CiscoSecure-Defined-ACL= <Name heruntergeladen>

Schlussfolgerung

Nachdem Sie jetzt alles über herunterladbare ACLs für Catalyst 1300 Switches wissen, lesen Sie den Artikel Herunterladbare ACLs für Catalyst 1300 Switches für die Schritte zu ihrer Konfiguration.

Weitere Informationen finden Sie im Administratorhandbuch für Catalyst 1300 und auf der Support-Seite für Cisco Catalyst Switches der Serie 1300.

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.