Catalyst 1300交換器中的可下載ACL概觀

目標

本文的目標是提供Catalyst 1300交換器中的可下載ACL(DACL)功能的概觀。

適用裝置 | 軟體版本

- Catalyst 1300 系列 | 4.1.6.54

簡介

動態ACL是根據策略或條件（如使用者帳戶組成員資格、一天中的時間等）分配給交換機埠的ACL。它們可能是由filter-ID或可下載ACL(DACL)指定的本地ACL。

可下載ACL是從思科ISE伺服器建立和下載的動態ACL。它們根據使用者身份和裝置型別動態應用訪問控制規則。DACL的優點是允許您為ACL建立一個中央儲存庫，因此您無需在每個交換機上手動建立它們。當使用者連線到交換機時，他們只需要進行身份驗證，交換機將從思科ISE伺服器下載適用的ACL。

目錄

DACL注意事項

在Catalyst 1300交換器上使用DACL時，請記住幾個注意事項。

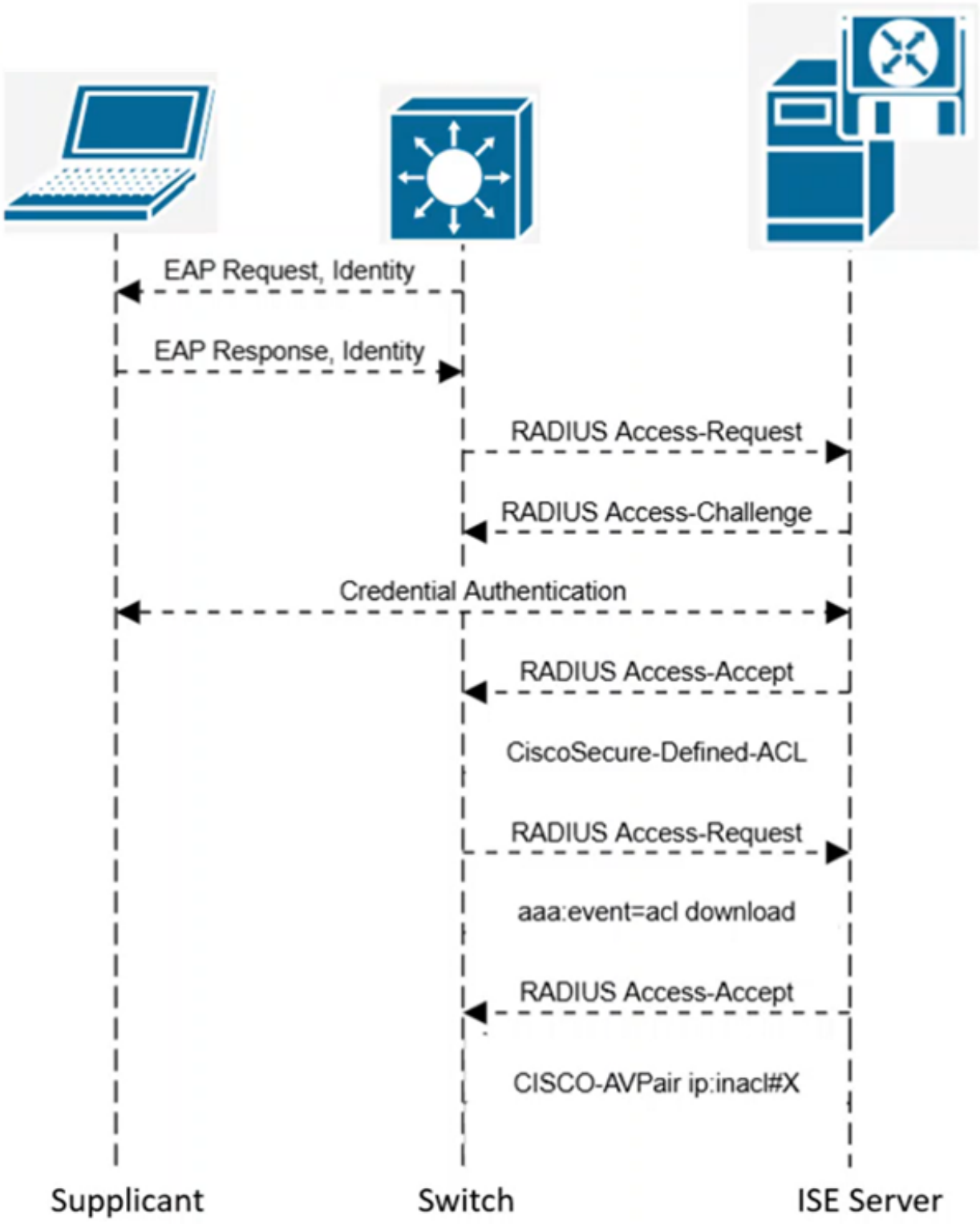
- 此功能是Catalyst 1300交換器獨有的；catalyst 1200交換器不支援這種設定。
- 應用了策略對映的介面不支援動態ACL。
    - 交換機不會傳送對ACL規則的訪問請求。
    - Supplicant客戶端將設定為Authenticated而不是Authorized狀態。
- 動態ACL與IP來源防護和（介面層級）安全性套件相關組態互相排斥
- 將動態ACL與堆疊式交換器一起使用時，需考慮以下幾點。
    - 如果主用裝置發生故障轉移，新的主用交換機將不會將DACL儲存在其本地記憶體中，並且需要重新下載所有DACL。

- 應用於作為客戶端系統身份驗證的一部分分配的介面的所有規則將被刪除。

- 如果您使用的是MAB(MAC Authentication Bypass)，則必須將MAC身份驗證型別設定為RADIUS（而不是預設的EAP方法）。
- ACL名稱長度
    - DACL:64個字元
    - 靜態：32個字元
- 動態ACL都是延伸型ACL。
- DACL使用的TCAM資源比您預期的要多。
- 可下載ACL會在沒有埠使用該ACL時自動刪除。
- 當沒有埠使用動態或可下載ACL時，為動態ACL建立的預設ACL將自動刪除。

DACL下載程式

- 作為標準802.1x身份驗證啟動。
- 使用者端通過驗證之後
    - ISE伺服器通過思科供應商AVPair - ACS傳送RADIUS Access-Accept:CiscoSecure-Defined-ACL = <ACL Name>
    - 交換器使用Cisco供應商AVPair傳送RADIUS存取要求 — aaa:event=acl-download
    - ISE伺服器向Cisco供應商AVPair-ip:inacl#<ACE條目的編號> = ACE傳送RADIUS訪問接受



可下載ACL名稱

在交換機上下載並分配給DACL的名稱與在ISE上建立的DACL的名稱不同。

例如，如果在ISE中建立名為Marketing_ACL的DACL，則下載時它可能顯示為#ACSACL#-IP-Marketing_ACL-57f6b0d4。

- ISE伺服器上的格式：<name> - ex:Marketing_ACL
- 下載到C1300交換機的格式
    - #ACSACL#-IP-<name>-<number>
    - 例如：#ACSACL#-IP-Marketing_ACL-57f6b0d4
- 名稱段
    - #ACSACL# - ISE新增的字首
    - IP — 表示ACL的型別(IP ACL)
    - <name> — 在ISE上建立的ACL的名稱
    - <number> — 版本號（ASCII十六進位制格式）
- 名稱長度必須小於或等於64個字元
- 封裝在Cisco-AVPair中：ACS:CiscoSecure-Defined-ACL= <已下載名稱>

結論

現在您已瞭解Catalyst 1300交換器中的可下載ACL，請檢視Catalyst 1300交換器中的可下載ACL文章，瞭解其設定步驟。

如需詳細資訊，請檢視Catalyst 1300管理指南和Cisco Catalyst 1300系列支援頁面。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。