Overview of Downloadable ACL in Catalyst 1300 Switches

Objective

The objective of this article is to provide you with an overview of downloadable ACL (DACL) feature in Catalyst 1300 switches.

Applicable Devices | Software Version

- Catalyst 1300 series | 4.1.6.54

Introduction

Dynamic ACLs are ACLs assigned to a switch port based off a policy or criteria such as user account group membership, time of day, and more. They could be local ACLs that are specified by filter-ID or downloadable ACLs (DACL).

Downloadable ACLs are dynamic ACLs that are created and downloaded from the Cisco ISE server. They dynamically apply access control rules based on user identity and device type. DACL has the benefit of allowing you to have one central repository for ACLs, so you don't need to manually create them on each switch. When a user connects to a switch, they just need to authenticate, and the switch will download the applicable ACLs from the Cisco ISE server.

Table of Contents

DACL Considerations

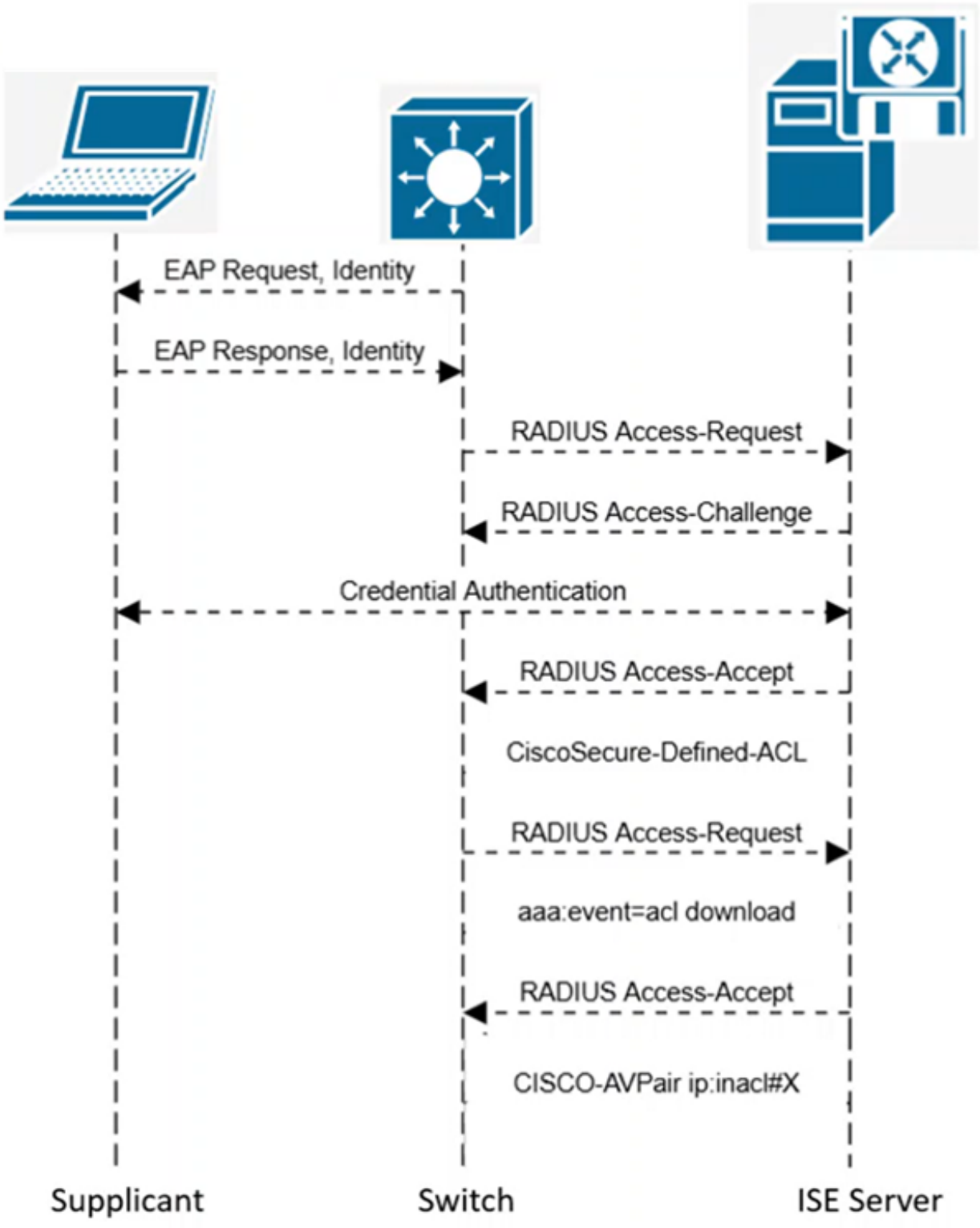
There are a few considerations to keep in mind when working with DACL on Catalyst 1300 switches.

- This feature is exclusive to the Catalyst 1300 switches; it is not supported on the Catalyst 1200 switches.
- Dynamic ACLs are not supported on interfaces with a Policy Map applied.
    - Switch will not send access-request for ACL rules.
    - Supplicant will be set to Authenticated but not Authorized state.

- Dynamic ACLs are mutually exclusive with IP Source Guard and (interface level) security-suite related configuration
- When using dynamic ACLs with stacked switches, there are some points to consider.
    - If the Active unit fails over, the new Active switch will not have the DACLs stored in its local memory and all DACLs need to be re-downloaded.
    - All rules applied to interfaces that were assigned as part of the client system's authentication will be removed.
- It is necessary to set MAC authentication Type to RADIUS (rather than the default EAP method) if you are using MAB (MAC Authentication Bypass).
- ACL name length
    - DACL: 64 characters
    - Static: 32 characters
- Dynamic ACLs are all extended ACLs.
- DACLs use more TCAM resources than you might expect.
- Downloadable ACLs are automatically deleted when no ports are using that ACL.
- The default ACL created for dynamic ACLs is automatically deleted when no ports are using dynamic or Downloadable ACLS.

DACL Download Process

- Starts as a standard 802.1x Authentication.
- After client has authenticated
    - ISE server sends RADIUS Access–Accept with Cisco Vendor AVPair – ACS: CiscoSecure-Defined-ACL = <ACL Name>
    - Switch sends RADIUS Access-Request with Cisco Vendor AVPair – aaa:event=acl-download
    - ISE Server sends RADIUS Access-Accept with Cisco Vendor AVPair-ip:inacl#<Number of the ACE entry> = ACE



Downloadable ACL Names

The name that is downloaded and assigned to the DACL on the switch is not the same as the DACL you create on ISE.

For example, if a DACL called Marketing_ACL is created in ISE, when it downloads it may

appear as #ACSACL#-IP-Marketing_ACL-57f6b0d4.

- Format on ISE server: <name> - ex: Marketing_ACL
- Format Downloaded to C1300 Switch
    - #ACSACL#-IP-<name>-<number>
    - ex: #ACSACL#-IP-Marketing_ACL-57f6b0d4
- Name Segments
    - #ACSACL# - Prefix added by ISE
    - IP – indicates type of ACL (IP ACL)
    - <name> - Name of the ACL created on ISE
    - <number> - version number in ASCII hex
- Name length must be less than or equal to 64 characters
- Encapsulated in *Cisco-AVPair: ACS:CiscoSecure-Defined-ACL= <Downloaded Name>*

Conclusion

Now that you know all about downloadable ACL in Catalyst 1300 switch, check out the article **Downloadable ACL in Catalyst 1300 Switches** for steps to configure it.

For more information, check out the **Catalyst 1300 Admin Guide** and the **Cisco Catalyst 1300 Series Support Page**.