

Descripción general de ACL descargable en switches Catalyst 1300

Objetivo

El objetivo de este artículo es proporcionarle una descripción general de la función de ACL descargable (DACL) en los switches Catalyst 1300.

Dispositivos aplicables | Versión de software

- Catalyst 1300 Series |4.1.6.54

Introducción

Las ACL dinámicas son ACL asignadas a un puerto de switch en función de una política o criterios como la pertenencia a grupos de cuentas de usuario, la hora del día, etc. Pueden ser ACL locales que se especifican mediante ID de filtro o ACL descargables (DACL).

Las ACL descargables son ACL dinámicas que se crean y descargan del servidor Cisco ISE. Aplican dinámicamente reglas de control de acceso basadas en la identidad del usuario y el tipo de dispositivo. DACL tiene la ventaja de que le permite tener un repositorio central para las ACL, por lo que no necesita crearlas manualmente en cada switch. Cuando un usuario se conecta a un switch, solo tiene que autenticarse y el switch descargará las ACL aplicables del servidor Cisco ISE.

Table Of Contents

- [Consideraciones sobre DACL](#)
- [Proceso de descarga de DACL](#)
- [Nombres de ACL descargables](#)

Consideraciones sobre DACL

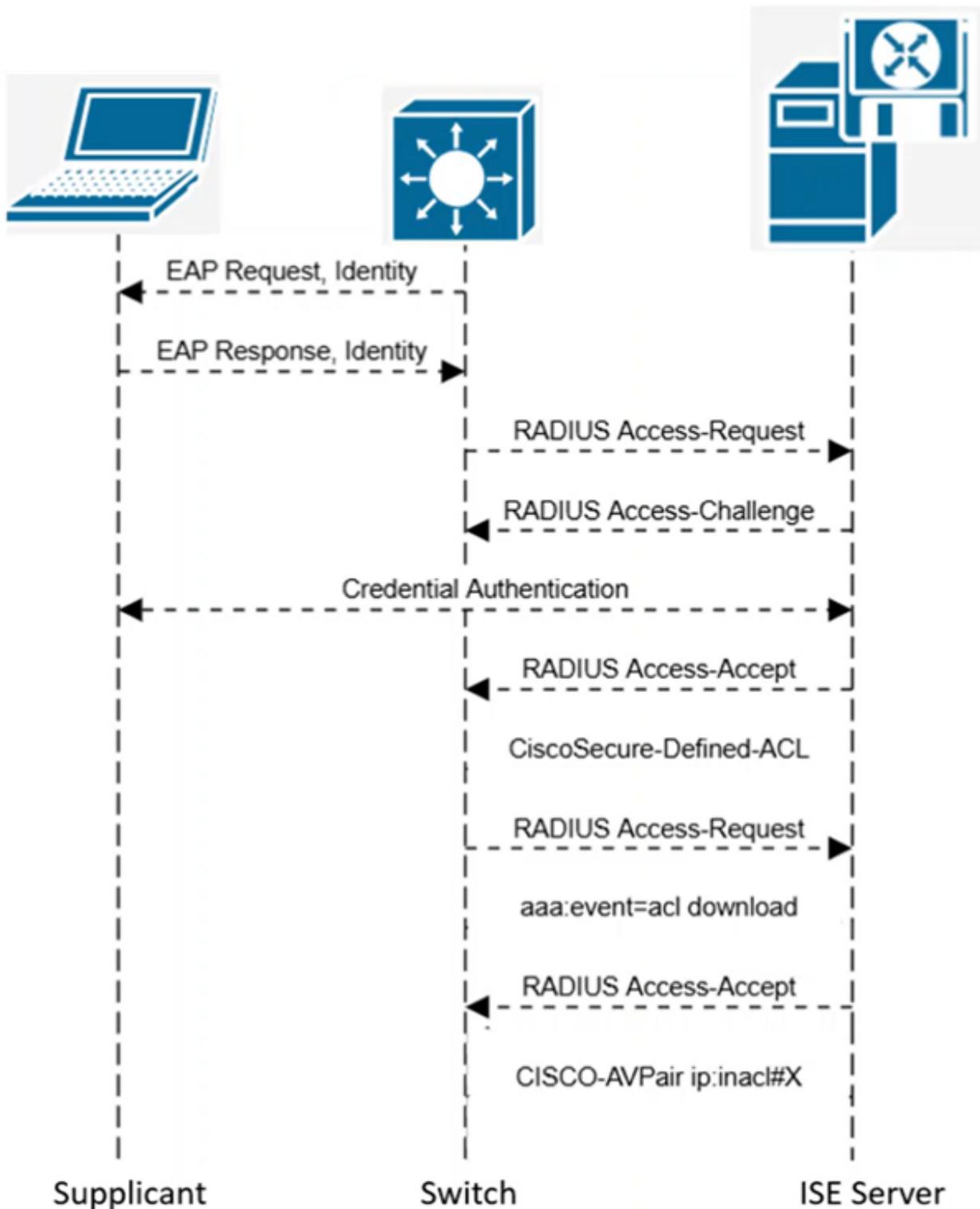
Hay algunas consideraciones que se deben tener en cuenta al trabajar con DACL en switches Catalyst 1300.

- Esta función es exclusiva de los switches Catalyst 1300; no es compatible con los switches Catalyst 1200.

- Las ACL dinámicas no se soportan en las interfaces con un Policy Map aplicado.
 - El switch no enviará una solicitud de acceso para las reglas ACL.
 - El suplicante se establecerá en el estado Autenticado pero no Autorizado.
- Las ACL dinámicas se excluyen mutuamente con IP Source Guard y la configuración relacionada con el conjunto de seguridad (nivel de interfaz)
- Cuando se utilizan ACL dinámicas con switches apilados, hay algunos puntos a considerar.
 - Si la unidad activa falla, el nuevo switch activo no tendrá las DACL almacenadas en su memoria local y todas las DACL deberán ser descargadas nuevamente.
 - Se eliminarán todas las reglas aplicadas a las interfaces que se asignaron como parte de la autenticación del sistema cliente.
- Es necesario establecer el tipo de autenticación MAC en RADIUS (en lugar del método EAP predeterminado) si utiliza MAB (omisión de autenticación MAC).
- Longitud del nombre ACL
 - DACL: 64 caracteres
 - Estática: 32 caracteres
- Las ACL dinámicas son todas ACL extendidas.
- Las DACL utilizan más recursos TCAM de lo que cabría esperar.
- Las ACL descargables se eliminan automáticamente cuando ningún puerto utiliza esa ACL.
- La ACL predeterminada creada para las ACL dinámicas se elimina automáticamente cuando ningún puerto utiliza ACL dinámicas o descargables.

Proceso de descarga de DACL

- Se inicia como una autenticación 802.1x estándar.
- Después de que el cliente se haya autenticado
 - El servidor ISE envía una aceptación de acceso RADIUS con el proveedor de Cisco AVPair - ACS: CiscoSecure-Defined-ACL = <ACL Name>
 - El switch envía una solicitud de acceso RADIUS con el proveedor de Cisco AVPair - aaa:event=acl-download
 - El servidor ISE envía la aceptación de acceso RADIUS con el proveedor de Cisco AVPair-ip:inacl#<Número de la entrada ACE> = ACE



Nombres de ACL descargables

El nombre que se descarga y se asigna a la DACL en el switch no es el mismo que la DACL que se crea en ISE.

Por ejemplo, si se crea una DACL denominada Marketing_ACL en ISE, cuando se

descarga puede aparecer como #ACSACL#-IP-Marketing_ACL-57f6b0d4.

- Formato en servidor ISE: <name> - por ejemplo: Marketing_ACL
- Formato descargado al switch C1300
 - #ACSACL#-IP-<nombre>-<número>
 - ej.: #ACSACL#-IP-Marketing_ACL-57f6b0d4
- Nombre de segmentos
 - #ACSACL# - Prefijo agregado por ISE
 - IP: indica el tipo de ACL (ACL IP).
 - <name>: nombre de la ACL creada en ISE
 - <number> - número de versión en hex ASCII
- La longitud del nombre debe ser menor o igual que 64 caracteres
- Encapsulado en Cisco-AVPair: ACS:CiscoSecure-Defined-ACL= <Nombre descargado>

Conclusión

Ahora que ya sabe todo sobre ACL descargable en el switch Catalyst 1300, consulte el artículo [ACL descargable en switches Catalyst 1300](#) para conocer los pasos para configurarla.

Para obtener más información, consulte la [Guía de administración de Catalyst 1300](#) y la [Página de soporte de Cisco Catalyst 1300 Series](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).