

Visão geral da ACL para download em switches Catalyst 1300

Objetivo

O objetivo deste artigo é fornecer uma visão geral do recurso de ACL para download (DACL) nos switches Catalyst 1300.

Dispositivos aplicáveis | Versão do software

- Catalyst 1300 Series | 4.1.6.54

Introdução

As ACLs dinâmicas são ACLs atribuídas a uma porta de switch com base em uma política ou em critérios, como a participação em grupos de contas de usuário, hora do dia e muito mais. Podem ser ACLs locais especificadas por ID de filtro ou ACLs para download (DACL).

As ACLs para download são ACLs dinâmicas criadas e baixadas do servidor Cisco ISE. Eles aplicam regras de controle de acesso dinamicamente com base na identidade do usuário e no tipo de dispositivo. A DACL tem a vantagem de permitir que você tenha um repositório central para ACLs, de modo que você não precisa criá-las manualmente em cada switch. Quando um usuário se conecta a um switch, ele só precisa se autenticar, e o switch fará o download das ACLs aplicáveis do servidor Cisco ISE.

Table Of Contents

- [Considerações sobre DACL](#)
- [Processo de download de DACL](#)
- [Nomes de ACL para download](#)

Considerações sobre DACL

Há algumas considerações a serem lembradas ao trabalhar com DACL em switches Catalyst 1300.

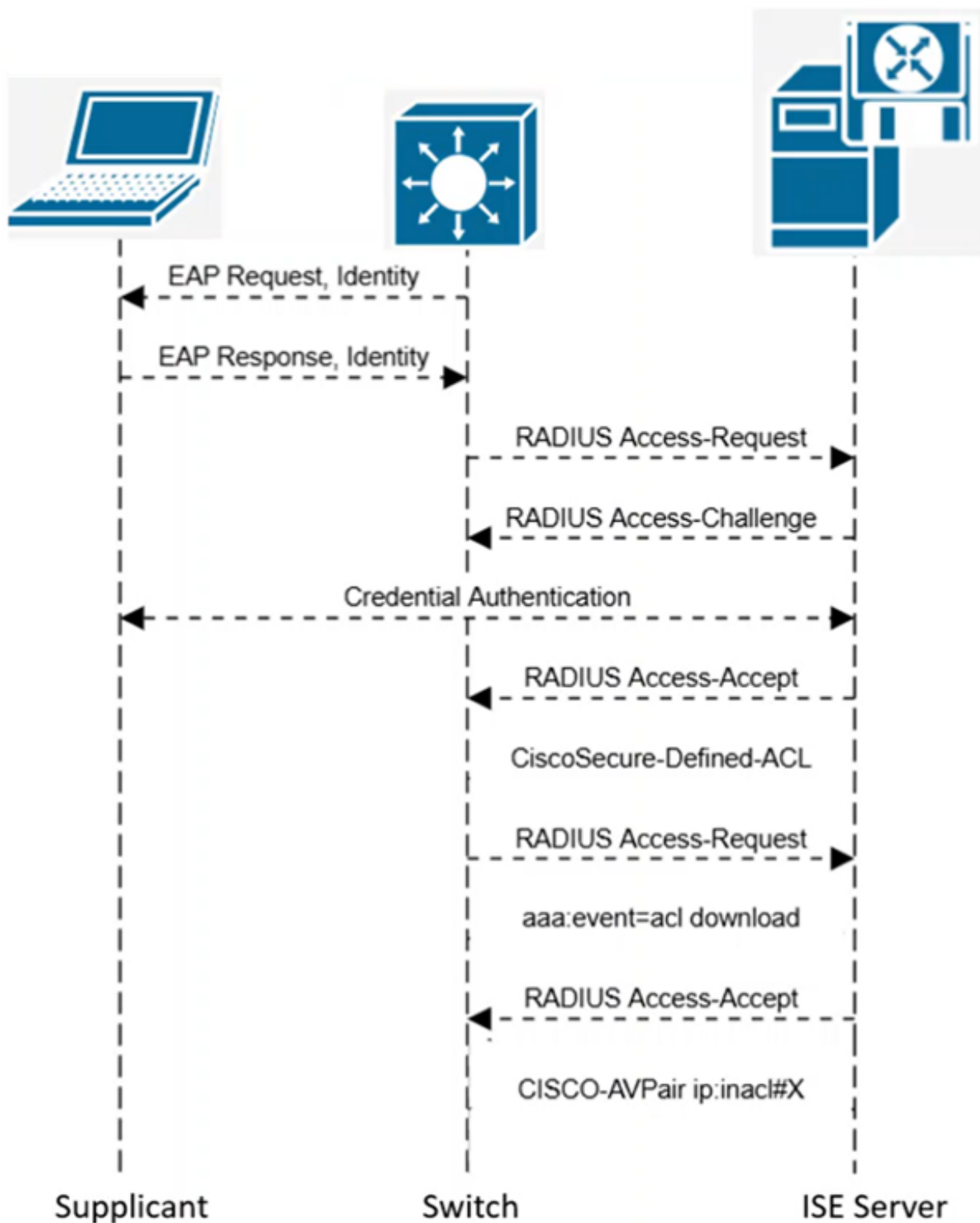
- Este recurso é exclusivo dos switches Catalyst 1300; não é suportado nos switches Catalyst

1200.

- As ACLs dinâmicas não são suportadas em interfaces com um mapa de política aplicado.
 - O switch não enviará solicitação de acesso para regras ACL.
 - O requerente será definido para o estado Autenticado, mas não Autorizado.
- As ACLs dinâmicas são mutuamente exclusivas com o IP Source Guard e a configuração relacionada ao conjunto de segurança (nível da interface)
- Ao usar ACLs dinâmicas com switches empilhados, há alguns pontos a serem considerados.
 - Se a unidade Ativa falhar, o novo switch Ativo não terá as DACLs armazenadas em sua memória local e todas as DACLs precisarão ser baixadas novamente.
 - Todas as regras aplicadas às interfaces que foram atribuídas como parte da autenticação do sistema cliente serão removidas.
- É necessário definir o Tipo de autenticação MAC como RADIUS (em vez do método EAP padrão) se você estiver usando MAB (MAC Authentication Bypass).
- comprimento do nome da ACL
 - DACL: 64 caracteres
 - Estático: 32 caracteres
- As ACLs dinâmicas são todas ACLs estendidas.
- As DACLs usam mais recursos de TCAM do que o esperado.
- As ACLs para download são excluídas automaticamente quando nenhuma porta está usando essa ACL.
- A ACL padrão criada para ACLs dinâmicas é automaticamente excluída quando nenhuma porta estiver usando ACLs dinâmicas ou que podem ser baixadas.

Processo de download de DACL

- Inicia como uma Autenticação 802.1x padrão.
- Depois que o cliente for autenticado
 - O servidor ISE envia RADIUS Access-Accept com o Cisco Vendor AVPair - ACS: CiscoSecure-Defined-ACL = <Nome da ACL>
 - O switch envia uma solicitação de acesso RADIUS com o Cisco Vendor AVPair - aaa:event=acl-download
 - O servidor ISE envia RADIUS Access-Accept com o Cisco Vendor AVPair- ip:inacl#<Número da entrada ACE> = ACE



Nomes de ACL para download

O nome que é baixado e atribuído à DACL no switch não é o mesmo que a DACL criada no ISE.

Por exemplo, se um DACL chamado Marketing_ACL for criado no ISE, quando ele

fizer o download, ele poderá aparecer como #ACSACL#-IP-Marketing_ACL-57f6b0d4.

- Formato no servidor ISE: <nome> - ex: ACL_Marketing
- Formato baixado para o switch C1300
 - #ACSACL#-IP-<nome>-<number>
 - ex.: #ACSACL#-IP-Marketing_ACL-57f6b0d4
- Segmentos de Nomes
 - #ACSACL# - Prefixo adicionado pelo ISE
 - IP - indica o tipo de ACL (ACL IP)
 - <nome> - Nome da ACL criada no ISE
 - <number> - número de versão em ASCII hexadecimal
- O nome deve ter 64 caracteres ou menos
- Encapsulado no Cisco-AVPair: ACS:CiscoSecure-Defined-ACL= <Nome do Download>

Conclusão

Agora que você sabe tudo sobre ACL transferível no switch Catalyst 1300, consulte o artigo [ACL transferível nos switches Catalyst 1300](#) para obter as etapas para configurá-la.

Para obter mais informações, consulte o [Guia de Administração do Catalyst 1300](#) e a [Página de Suporte do Cisco Catalyst 1300 Series](#).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.