Catalyst 1300スイッチのダウンロード可能ACLの概要

目的

この記事の目的は、Catalyst 1300スイッチのDownloadable ACL(DACL)機能の概要を説明することです。

該当するデバイス|ソフトウェアバージョン

- Catalyst 1300シリーズ| 4.1.6.54

はじめに

ダイナミックACLは、ポリシーまたはユーザアカウントグループメンバーシップ、時間帯などの基準に基づいて、スイッチポートに割り当てられるACLです。これらは、filter-IDまたはdownloadable ACL(DACL)で指定されたローカルACLである可能性があります。

ダウンロード可能ACLは、Cisco ISEサーバから作成およびダウンロードされるダイナミックACLです。ユーザIDとデバイスタイプに基づいて、アクセスコントロールルールを動的に適用するDACLには、ACLの中央リポジトリを1つ作成できるという利点があるため、各スイッチでACLを手動で作成する必要はありません。ユーザがスイッチに接続する際に必要なのは認証だけで、スイッチはCisco ISEサーバから該当するACLをダウンロードします。

目次

DACLの考慮事項

Catalyst 1300スイッチでDACLを使用する際には、いくつかの注意点があります。

- この機能はCatalyst 1300スイッチ専用で、Catalyst 1200スイッチではサポートされていません。
- ダイナミックACLは、ポリシーマップが適用されたインターフェイスではサポートされません。

- スイッチがACLルールのアクセス要求を送信しない。
- サプリカントは認証済みであるが承認済みではない状態に設定される

- ダイナミックACLは、IPソースガード(IPSG)および（インターフェイスレベル）セキュリティスイート関連の設定と相互排他的です
- スタックされたスイッチでダイナミックACLを使用する場合は、考慮すべき点がいくつかあります。

  - アクティブユニットがフェールオーバーすると、新しいアクティブスイッチのローカルメモリにDACLが保存されず、すべてのDACLを再度ダウンロードする必要があります。
  - クライアントシステムの認証の一部として割り当てられたインターフェイスに適用されたすべてのルールが削除されます。

- MAB（MAC認証バイパス）を使用している場合は、（デフォルトのEAP方式ではなく）MAC認証タイプをRADIUSに設定する必要があります。
- ACL名長

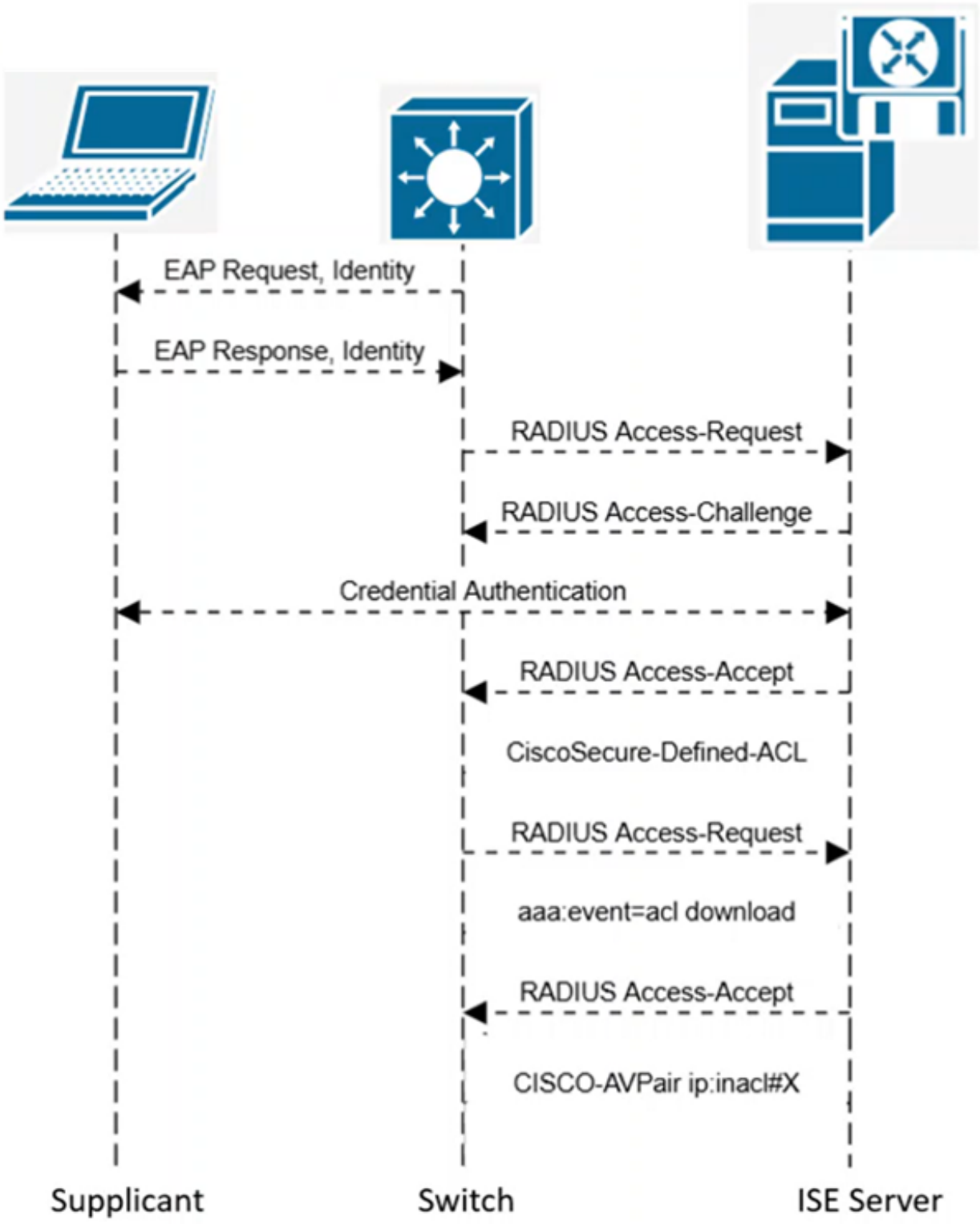
  - DACL:64文字
  - スタティック：32文字

- ダイナミックACLはすべて拡張ACLです。
- DACLは、予想よりも多くのTCAMリソースを使用します。
- ダウンロード可能ACLは、そのACLを使用しているポートがなくなると自動的に削除されます。
- ダイナミックACL用に作成されたデフォルトACLは、ダイナミックACLまたはダウンロード可能ACLを使用しているポートがない場合に自動的に削除されます。

DACLダウンロードプロセス

- 標準の802.1x認証として起動します。
- クライアントが認証した後

  - ISEサーバがCisco Vendor AVPairを使用してRADIUS Access-Acceptを送信：ACS:CiscoSecure-Defined-ACL = <ACL Name>
  - スイッチがCisco Vendor AVPairでRADIUS Access-Requestを送信：aaa:event=acl-download
  - ISEサーバがRADIUS Access-AcceptをCisco Vendor AVPair-ip:inacl#<Number of the ACE entry> = ACEで送信する



ダウンロード可能なACL名

ダウンロードされてスイッチのDACLに割り当てられる名前は、ISEで作成するDACLと同じではありません。

たとえば、Marketing_ACLという名前のDACLがISEで作成されている場合、ダウン口

ード時に#ACSACL#-IP-Marketing_ACL-57f6b0d4と表示されることがあります。

- ISEサーバの形式：<name> – 例：Marketing_ACL
- C1300スイッチにダウンロードされたフォーマット
    - #ACSACL#-IP-<name>-<number>
    - 例： #ACSACL#-IP-Marketing_ACL-57f6b0d4
- 名前セグメント
    - #ACSACL#:ISEによって追加されるプレフィックス
    - IP:ACLのタイプを示します(IP ACL)。
    - <name>:ISEで作成されたACLの名前
    - <number>:ASCII 16進数のバージョン番号
- 名前の長さは64文字以下でなければなりません
- Cisco-AVPair:ACS:CiscoSecure-Defined-ACL= <Downloaded Name>にカプセル化されます。

結論

Catalyst 1300スイッチのダウンロード可能ACLについてはすべて理解できたので、「Catalyst 1300スイッチのダウンロード可能ACL」を参照して設定手順を確認してください。

詳細については、『Catalyst 1300管理ガイド』および『Cisco Catalyst 1300シリーズサポートページ』を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。