ISEはマイネットワークアクセスデバイスをサポートしますか。

内容

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)とネットワークアクセスデバイス(NAD)の互換性を確認する方法について説明します。

ISEがRADIUSおよびTACACSプロトコルをサポート

ネットワークデバイスが標準のRADIUSおよびTACACSプロトコルを使用してアクセスコントロール要求を発行できる場合、ISEはそれをサポートできます。

ISEは、ネットワークデバイスのハードウェアおよびソフトウェアがサポートする強制メカニズムを使用してアクセス制御を実行するために、RADIUSをサポートします。

IEEE 802.1X標準でポートベースのアクセス制御を行うネットワークデバイスの機能は、ソフトウェアです。ハードウェアに依存する場合もよくあります。RADIUSをサポートするだけでは、ネットワークデバイスがMAC認証バイパス(MAB)、RADIUS認可変更(CoA) [RFC-5176]、レイヤ3/4アクセスコントロールリスト(ACL)、ドメインベースのACLなどの多くの有用な適用機能ををサポートするわけではありませんs、URLリダイレクション、またはCisco TrustSecを使用したソフトウェア定義のセグメンテーション。特定のネットワークデバイスが何に対応しているかを常に把握することはできず、ベンダーや製品チームに調査を依頼する必要があります。

人々が尋ねるとISEはネットワークデバイスをサポートしていますか。つまり、ISEは、この古い安価なスイッチでも、これらの最新のアクセスコントロール機能をすべて提供できますか。

ISEは、ゲスト、BYOD、およびポスチャフローの処理に必要な同様の機能を提供するために、SNMP CoAや認証VLANなどの機能を提供します。

ISE互換性ガイド

ISE互換性ガイドを必ず**確認し**て、ISEリリースごとにQuality Assurance(QA)チームが検証済みであることを確認してください。

ISEのネットワークデバイス機能

ISE機能を提供するために通常必要な最新のネットワークデバイス機能を次に示します。

ISE機能	ネットワークデバイスの機能
[AAA]	802.1X、MAB、VLAN割り当て、ダウンロード可能ACL
プロファイリング	RADIUS CoAおよびプロファイリングプローブ
BYOD	RADIUS CoA、URLリダイレクション+ SessionID
ゲスト	RADIUS CoA、URLリダイレクション+ SessionID、ローカルWeb認証
ゲスト発信URL	RADIUS CoA、URLリダイレクション+ SessionID、ローカルWeb認証
ポスチャ	RADIUS CoA、URLリダイレクション+ SessionID
MDM	RADIUS CoA、URLリダイレクション+ SessionID
TrustSec	SGTの分類

ネットワークデバイスにISE機能の機能がすべて備わっていない場合はどうすればよいでしょうか。

ネットワークアクセスデバイス(NAD)プロファイルを作成します。

ネットワークデバイスの機能を知る方法

検証済みのハードウェアとソフトウェアの組み合わせの機能については、ISE互換性ガイドに記載されています。その他すべてのベンダーのWebサイト、製品ドキュメント、フォーラムなどで調査する必要があります。場合によっては、ラボで再生するだけで、機能の仕組みや機能の違いを確認したり、さまざまな機能の組み合わせに対応するネットワークデバイスプロファイルを作成したりすることがあります。

『ISE Compatibility Guide』にハードウェアまたはソフトウェアが表示されない

ハードウェアモデルまたはソフトウェアリリースが明示的にリストされていないからといって、動作しないということではありません。ISEで検証していないということだけです。『ISE Compatibility Guides』の「Supported Network Access Devices」セクションには、ベンダーやモデルに関わらず、ISEがRADIUSをサポートすると記載されています。

Cisco ISEは、標準ベースの認証に共通のRADIUS動作（Cisco IOS 12.xと同様）を実装する、シスコまたトワークアクセスデバイス(NAD)との相互運用性をサポートします。

ISEは、RADIUS、関連するRFC標準、およびTACACS+などのプロトコル標準をサポートしています。使用しているネットワークデバイスがRADIUSまたはTACACS+をサポートしている場合、ISEはそれをサポートできます。

シスコ製デバイスとシスコ製以外のデバイスの両方が表示されない理由は多数あります。

- QAチームは、すべてのハードウェアとソフトウェアの組み合わせをISEリリースごとにテストする余裕がありません。
- **新しいハードウェアプラ**トを取得してテストする必要があります。通常、ハードウェアリリースから6 ~ 9ヵ月以内に行われます。
- **ハードウェアファミリのすべてのモデル**は検証されません。1つのモデルが選択され、ハードウェアファミリを表すために使用されます。
- **すべてのソフトウェアリリース**は検証されません。プラットフォームチームが推奨するリリース済みプラットフォームソフトウェアバージョンが1つ選択されます。これは、QA検証計

画の実際のISEリリースの数ヶ月前です。
- 古いISEリリースは、新しいネットワークデバイスソフトウェアではテストされませんが、標準に従ってテストする必要があります。

ISEで実行できる内容は、ネットワークデバイスのハードウェアおよびソフトウェアの機能によって決まります。実稼働環境に導入する前に、ISEを使用してラボでネットワークデバイスのハードウェアとソフトウェアを試すことを常に推奨します。そのため、期待どおりに動作することを確信できます。

ISEネットワークアクセスデバイス(NAD)プロファイル

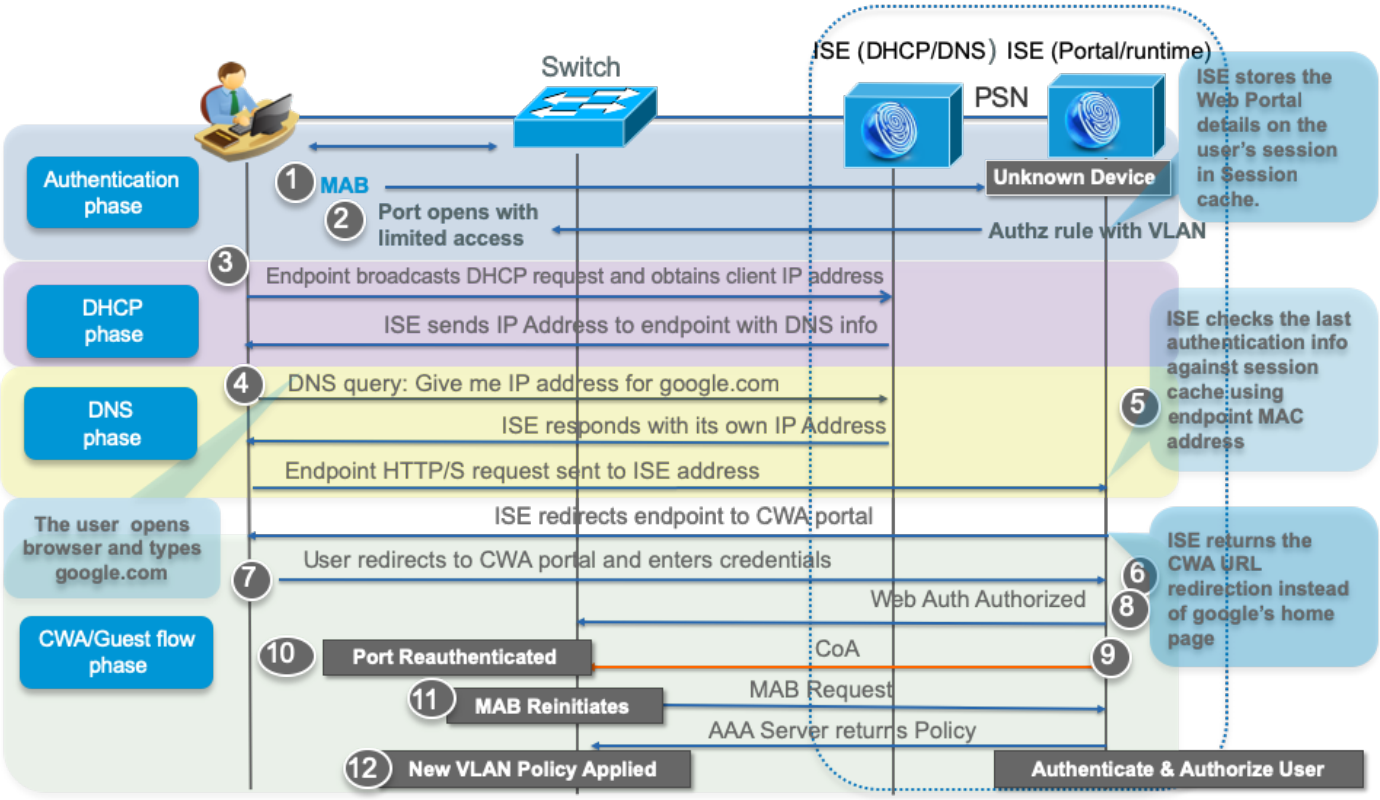
次の場合：

- シスコ以外のハードウェア
- 安価なローエンドネットワークデバイスハードウェア
- 古いネットワークデバイスハードウェア
- 古いネットワークデバイスソフトウェア

その後、ISEのサードパーティNADプロファイルと構成を使用するか、独自のカスタムNADプロファイルを作成できます。NADプロファイルを使用すると、RADIUS CoAのカスタムポート上にあるか、URLリダイレクションの代わりに認証VLANを使用する必要があるかに関係なく、ISEがネットワークデバイスと通信する方法を完全にカスタマイズできます。

認証VLANのサポート

802.1Xを使用できない古いレガシースイッチがある場合、ISEは認証VLANを使用してエンドポイントを制御できます。これは、ユーザが認証できるWebポータルにHTTPトラフィックをリダイレクトするためにDNSとDHCPを使用する、非常に粗い制御方式です。詳細については、『ISE Administrators Guides』の「Cisco ISEでのサードパーティ製ネットワークデバイスのサポート」を参照してください。



認証VLANの使用に関する問題

- ポートごとに複数のデバイスを制御することはできません。
- L2 VLANではトラフィックフィルタリングが非常に粗く、VACLまたはVRFを除き、L3/4 IP/プロトコル/ポート制御は行われません。
- VLAN内にEast/Westセグメンテーションがない場合、VLAN内の他のエンドポイントにマルウェアが簡単に拡散されます（信頼できないエンドポイントでも信頼できるエンドポイントでも）。