ISE是否支援我的網路訪問裝置？

目錄

簡介

本文說明如何檢查思科身份服務引擎(ISE)與您的網路訪問裝置(NAD)的相容性。

ISE支援RADIUS和TACACS協定

如果您的網路裝置可以使用標準RADIUS和TACACS通訊協定發出存取控制要求，則ISE可支援它！

ISE支援RADIUS使用網路裝置硬體和軟體支援的任何實施機制執行訪問控制。

給定網路裝置通過IEEE 802.1X標準執行埠型訪問控制的功能是軟體的，而且通常依賴於硬體！僅僅支援RADIUS並不表示網路裝置支援許多有用的執行功能，例如MAC驗證略過(MAB)、RADIUS授權變更(CoA) [RFC-5176]、第3/4層存取控制清單(ACL)、網域型ACL、URL重新導向或使用Cisco TrustSec進行軟體定義分段。您不能總是告訴您任何給定網路裝置具備的能力，您可能需要與供應商或產品團隊一起研究。

當人們提出要求時；ISE是否支援我的網路裝置？他們的意思是，ISE能否為我提供所有這些現代訪問控制功能，即使使用這個老舊且廉價的交換機？

對於這些較舊且價格較低的交換機，ISE提供SNMP CoA和身份驗證VLAN等功能，以提供處理訪客、BYOD和狀態流所需的類似功能。

ISE相容性指南

請始終檢視**ISE相容性指南**，檢視我們的品質保證(QA)團隊對每個ISE版本進行了哪些驗證。

ISE網路裝置功能

以下是交付ISE功能通常所需的現代網路裝置功能：

ISE功能	網路裝置功能
AAA	802.1X、MAB、VLAN分配、可下載ACL
分析	RADIUS CoA和分析探測

自帶裝置	RADIUS CoA，URL重新導向+作業階段ID
訪客	RADIUS CoA，URL重新導向+ SessionID，本地Web驗證
訪客源URL	RADIUS CoA，URL重新導向+ SessionID，本地Web驗證
狀態	RADIUS CoA，URL重新導向+作業階段ID
MDM	RADIUS CoA，URL重新導向+作業階段ID
TrustSec	SGT分類

如果您的網路裝置沒有ISE功能的所有功能，您會怎麼做？

建立網路存取裝置(NAD)設定檔。

如何瞭解網路裝置的功能？

我們的ISE相容性指南中提供了經驗證的硬體和軟體組合的功能。對於所有其他使用者，您需要在供應商的網站、產品文檔、論壇等中進行這方面的研究。有時，您可能只需在實驗室中玩著，瞭解哪些功能有效，哪些不能，然後針對不同的功能組合建立網路裝置配置檔案。

無法在ISE相容性指南中看到您的硬體或軟體

僅僅因為未明確列出硬體型號或軟體版本，並不意味著它無法正常工作 — 只是您尚未使用ISE對其進行驗證！ISE相容性指南的**支援的網路訪問裝置**部分宣告ISE支援RADIUS，無論供應商或型號如何：

思科ISE支援與任何實施常見RADIUS行為（類似於思科IOS 12.x）的思科或非思科RADIUS客戶端網路接入(NAD)的互操作性，用於基於標準的身份驗證。

ISE支援RADIUS、其關聯的RFC標準和TACACS+等協定標準。如果您的網路裝置支援RADIUS和/或TACACS+，則ISE可支援它！

可能未列出思科和非思科裝置的原因有很多：

- 我們的QA團隊無法承受使用每個ISE版本測試每個硬體和軟體組合的費用。
- **必須購買並**測試新的硬體平台，這通常在硬體發佈後的6-9個月內發生。
- **每個硬體系列的型號**都不會經過驗證 — 選擇一個型號，然後將其用於表示該硬體系列。
- **每個軟體版**本均未驗證 — 平台團隊推薦的一個發佈平台軟體版本被選定，這比用於品質驗證計畫的實際ISE版本早幾個月。
- 較舊的ISE版本不能使用較新的網路裝置軟體進行測試，但仍應根據標準進行測試。

您使用ISE可以執行的操作具體取決於網路裝置的硬體和軟體功能。我們始終建議您在實驗室中嘗試使用ISE的網路裝置硬體和軟體，然後再將其部署到生產環境中，以便您確信其行為與預期一致。

ISE網路訪問裝置(NAD)配置檔案

如果有：

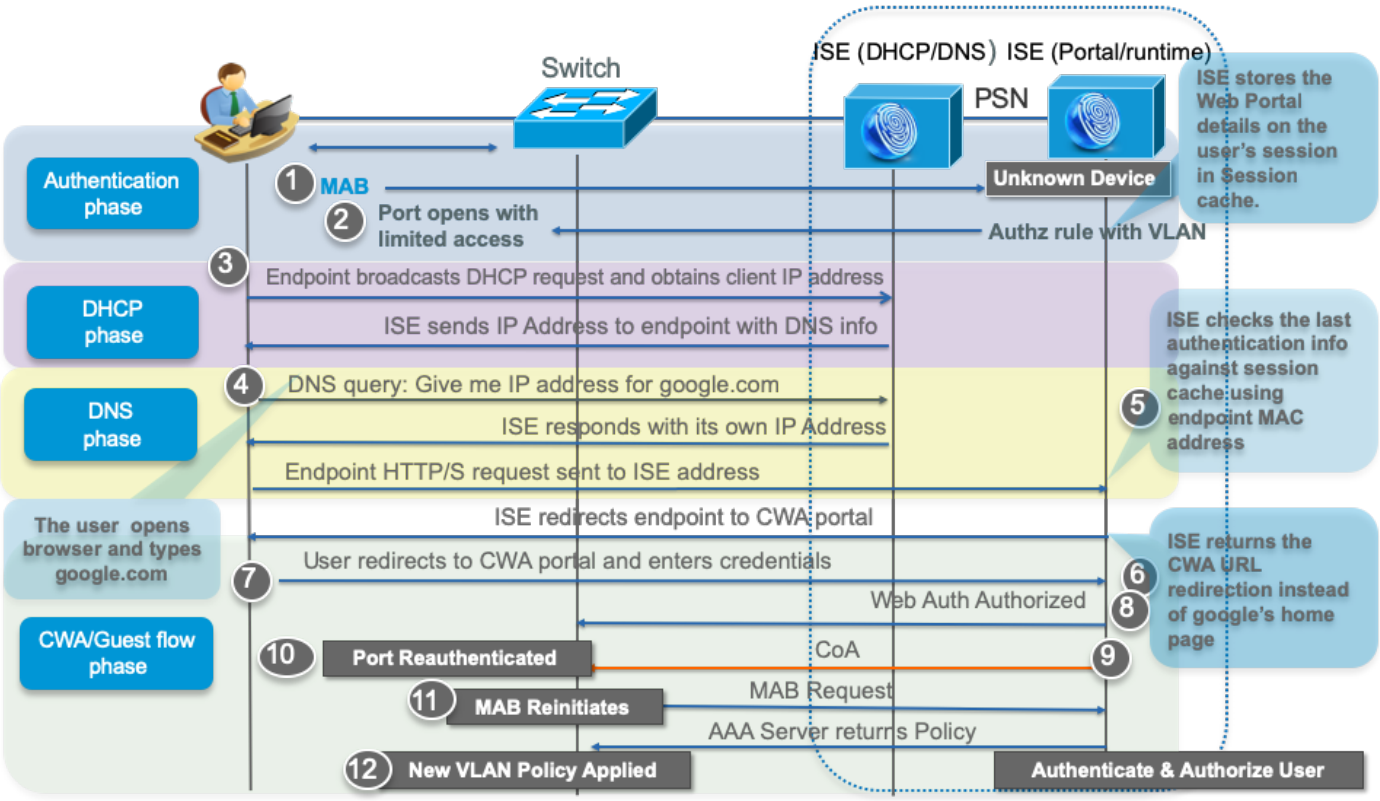
- 非思科硬體
- 廉價的低端網路裝置硬體
- 舊網路裝置硬體
- 舊網路裝置軟體

然後您可以使用我們的ISE第三方NAD配置檔案和配置，或建立您自己的自定義NAD配置檔案。使

用NAD配置檔案，您可以完全自定義ISE與網路裝置的通訊方式，無論其位於RADIUS CoA的自定義埠上，還是需要使用身份驗證VLAN而不是URL重定向。

驗證VLAN支援

如果您有一些不能使用802.1X的舊式交換機，ISE確實能夠使用身份驗證VLAN控制終端。這是一種非常粗糙的控制方法，使用DNS和DHCP將HTTP流量重定向到使用者可能進行身份驗證的Web門戶。有關詳細資訊，請參閱ISE管理員指南中的Cisco ISE中的第三方網路裝置支援(Third-Party Network Device Support in Cisco ISE)。



使用驗證VLAN時出現問題

- 不能控制每個埠的多個裝置。
- 第2層VLAN的流量過濾非常粗糙 — 除了VACL或VRF外，沒有第3/4層IP/協定/埠控制。
- VLAN中沒有East/West分段意味著惡意軟體很容易傳播到VLAN中的其他終端，無論是不受信任還是受信任。