ISE是否支持我的网络访问设备？

目录

简介

- ISE支持RADIUS和TACACS协议

ISE兼容性指南

- ISE的网络设备功能
- 您如何了解网络设备的功能？
- 在ISE兼容性指南中看不到您的硬件或软件

ISE网络访问设备(NAD)配置文件

身份验证VLAN支持

- 使用身份验证VLAN时出现问题

简介

本文档介绍如何检查思科身份服务引擎(ISE)与您的网络接入设备(NAD)的兼容性。

ISE支持RADIUS和TACACS协议

如果您的网络设备可以使用标准RADIUS和TACACS协议发出访问控制请求，则ISE可以支持它！

ISE支持RADIUS使用网络设备硬件和软件支持的任何实施机制执行访问控制。

给定网络设备通过IEEE 802.1X标准执行基于端口的访问控制功能是软件功能，而且通常依赖于硬件！仅支持RADIUS并不意味着网络设备支持许多有用的实施功能，例如MAC身份验证绕行(MAB)、RADIUS授权更改(CoA) [RFC-5176]、第3/4层访问控制列表(ACL)、基于域的ACL、URL重定向或使用Cisco TrustSec的软件定义分段。您不能总是告诉您任何给定网络设备都具备的能力，您可能需要与供应商或产品团队一起研究。

当人们提出要求时；ISE是否支持我的网络设备？他们的意思是， ISE能否提供所有这些现代访问控制功能，即使使用这种老式且价格低廉的交换机？

对于这些较旧且较便宜的交换机，ISE提供SNMP CoA和身份验证VLAN等功能，以提供处理访客、BYOD和安全评估流程所需的类似功能。

ISE兼容性指南

请务必查看ISE兼容性指南，查看我们的质量保证(QA)团队对每个ISE版本进行了哪些验证。

ISE的网络设备功能

提供ISE功能通常需要以下现代网络设备功能：

ISE功能	网络设备功能

AAA	802.1X、MAB、VLAN分配、可下载ACL
分析	RADIUS CoA和分析探针
自带设备	RADIUS CoA、URL重定向+会话ID
访客	RADIUS CoA、URL重定向+会话ID、本地网络身份验证
访客源URL	RADIUS CoA、URL重定向+会话ID、本地网络身份验证
状态	RADIUS CoA、URL重定向+会话ID
MDM	RADIUS CoA、URL重定向+会话ID
Trustsec	SGT分类

如果您的网络设备没有ISE功能的所有功能，您会怎么做？

创建网络接入设备(NAD)配置文件。

您如何了解网络设备的功能？

经验证的硬件和软件组合的功能可在我们的ISE兼容性指南中方便地记录。对于所有其他用户，您需要在供应商的网站、产品文档、论坛等上进行这方面的研究。有时，您可能只需在实验中播放，了解哪些功能有效，哪些不能，然后针对不同的功能组合创建网络设备配置文件了。

在ISE兼容性指南中看不到您的硬件或软件

仅仅因为未明确列出硬件型号或软件版本，并不意味着它不会工作 — 只是您尚未使用ISE验证它！ISE兼容性指南的支持的网络访问设备部分说明ISE支持RADIUS，无论供应商或型号如何：

> 思科ISE支持与任何实施常见RADIUS行为（类似思科IOS 12.x）的思科或非思科RADIUS客户端网络接入设备(NAD)的互操作性，以进行基于标准的身份验证。

ISE支持RADIUS、其关联的RFC标准和TACACS+等协议标准。如果您的网络设备支持RADIUS和/或TACACS+，则ISE可以支持它！

可能未列出思科和非思科设备的原因有很多：

- 我们的QA团队承受不起在每个ISE版本中测试每个硬件和软件组合的成本。
- 必须购买并测试新硬件平台，通常在硬件发布后的6-9个月内进行。
- 每个硬件系列的型号都不会经过验证 — 选择一个型号，然后将其用于表示硬件系列。
- 每个软件版本均未经过验证 — 在实际ISE版本进行QA验证规划几个月前，将选择平台团队推荐的一个已发布平台软件版本。
- 较旧的ISE版本未使用较新的网络设备软件进行测试，但仍应根据标准进行测试。

ISE的具体功能取决于网络设备的硬件和软件功能。我们始终建议您先在实验室中尝试使用ISE的网络设备硬件和软件，然后再将其部署到生产环境中，这样您就可以确信其行为与预期一致。

ISE网络访问设备(NAD)配置文件

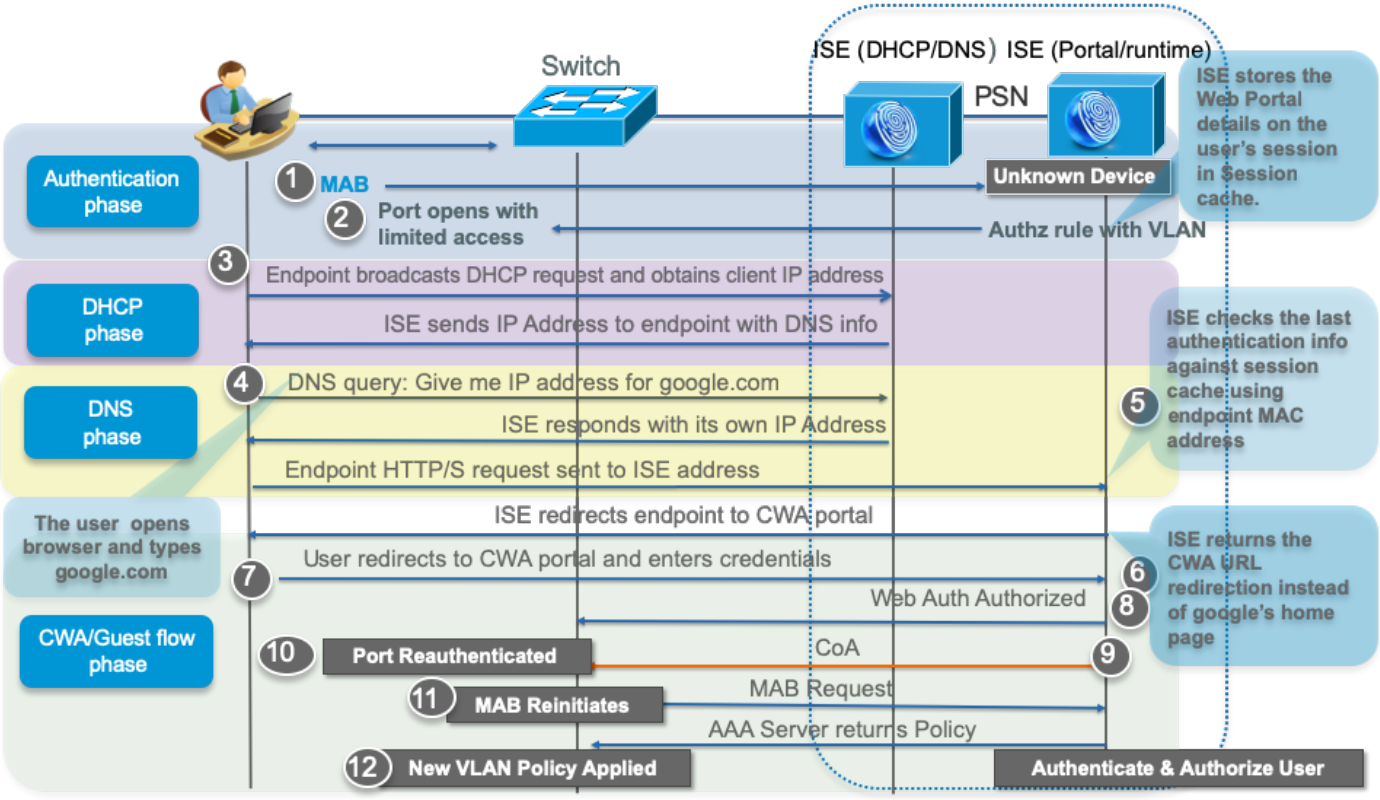
如果有：

- 非思科硬件
- 价格低廉的低端网络设备硬件
- 旧网络设备硬件
- 旧网络设备软件

然后，您可以使用我们的ISE第三方NAD配置文件和配置，或创建您自己的自定义NAD配置文件。使用NAD配置文件，您可以完全自定义ISE与网络设备的通信方式，无论它位于RADIUS CoA的自定义端口上，还是需要使用身份验证VLAN而不是URL重定向。

身份验证VLAN支持

如果您有一些不支持802.1X的旧式交换机，ISE确实能够使用身份验证VLAN控制终端。这是一种非常粗略的控制方法，它使用DNS和DHCP将HTTP流量重定向到用户可能进行身份验证的Web门户。有关详细信息，请参阅ISE Administrators Guides中的Third-Party Network Device Support in Cisco ISE。



使用身份验证VLAN时出现问题

- 您不能控制每个端口的多个设备。
- 第2层VLAN的流量过滤非常粗糙 — 除VACL或VRF外，不进行L3/4 IP/协议/端口控制。
- VLAN内没有East/West分段意味着恶意软件很容易传播到VLAN内的其他终端，无论是不受信任还是受信任。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。