ISE prend-il en charge mon périphérique d'accès réseau ?

Contenu

Introduction

Ce document décrit comment vérifier la compatibilité de Cisco Identity Services Engine (ISE) avec votre périphérique d'accès au réseau (NAD).

ISE prend en charge les protocoles RADIUS et TACACS

Si votre périphérique réseau peut émettre des demandes de contrôle d'accès à l'aide des protocoles RADIUS et TACACS standard, ISE peut le prendre en charge !

ISE prend en charge RADIUS pour effectuer le contrôle d'accès avec les mécanismes d'application pris en charge par le matériel et le logiciel du périphérique réseau.

Les capacités d'un périphérique réseau donné pour effectuer un contrôle d'accès basé sur les ports avec la norme IEEE 802.1X sont logicielles et souvent dépendantes du matériel ! La simple prise en charge de RADIUS ne signifie pas que le périphérique réseau prend en charge de nombreuses fonctionnalités d'application utiles, telles que MAB (MAC Authentication Bypass), RADIUS Change of Authorization (CoA) [RFC-5176], listes de contrôle d'accès (ACL) de couche 3/4, listes de contrôle d'accès basées sur le domaine, redirection d'URL ou segmentation définie par logiciel avec Cisco TrustSec. Vous ne pouvez pas toujours vous dire de quoi un périphérique réseau donné est capable et vous devrez peut-être faire des recherches avec le fournisseur ou l'équipe de produits.

Quand les gens demandent ; ISE prend-il en charge mon périphérique réseau ? Ce qu'ils veulent dire, est-ce que ISE peut me donner toutes ces fonctionnalités de contrôle d'accès modernes même avec ce vieux commutateur peu coûteux ?

Pour ces commutateurs plus anciens et moins coûteux, ISE propose des fonctionnalités telles que SNMP CoA et le VLAN d'authentification pour fournir des fonctionnalités similaires nécessaires pour gérer le flux invité, BYOD et Posture.

Guides de compatibilité ISE

Vérifiez toujours les guides de compatibilité ISE pour voir ce que notre équipe d'assurance qualité (QA) a validé pour chaque version ISE.

Fonctionnalités des périphériques réseau pour ISE

Il s'agit de fonctions de périphériques réseau modernes généralement requises pour fournir des fonctionnalités ISE :

Fonctionnalité ISE	Fonctionnalités des périphériques réseau
AAA	802.1X, MAB, affectation VLAN, listes de contrôle d'accès téléchargeables
Profilage	CoA RADIUS et probes de profilage
BYOD	CoA RADIUS, redirection d'URL + ID de session
Invité	CoA RADIUS, redirection URL + ID de session, authentification Web locale
URL d'origine de l'invité	CoA RADIUS, redirection URL + ID de session, authentification Web locale
Posture	CoA RADIUS, redirection d'URL + ID de session
MDM	CoA RADIUS, redirection d'URL + ID de session
TrustSec	Classification SGT

Que faites-vous si votre périphérique réseau ne dispose pas de toutes les fonctionnalités de la fonctionnalité ISE ?

Créez un profil NAD (Network Access Device).

Comment connaissez-vous les fonctionnalités de vos périphériques réseau ?

Les fonctionnalités des combinaisons matérielles et logicielles validées sont facilement documentées dans nos guides de compatibilité ISE. Pour tous les autres, vous devez effectuer des recherches sur les sites Web des fournisseurs, sur la documentation produit, sur les forums, etc. Parfois, vous n'avez qu'à jouer dans votre laboratoire pour savoir ce qui fonctionne et ce qui ne fonctionne pas et créer un profil de périphérique réseau pour les différentes combinaisons de fonctionnalités.

Impossible de voir votre matériel ou logiciel dans le guide de compatibilité ISE

Ce n'est pas parce qu'un modèle matériel ou une version logicielle n'est pas explicitement répertorié qu'il ne fonctionnera pas, mais seulement parce que vous ne l'avez pas validé avec ISE ! La section **Périphériques d'accès au réseau pris en charge** des guides de compatibilité ISE indique qu'ISE prend en charge RADIUS, quel que soit le fournisseur ou le modèle :

> Cisco ISE prend en charge l'interopérabilité avec tout périphérique d'accès réseau client (NAD) RADIUS ou non Cisco qui met en oeuvre un comportement RADIUS commun (similaire à Cisco IOS 12.x) pour l'authentification basée sur des normes.

ISE prend en charge les normes de protocole telles que RADIUS, ses normes RFC associées, et TACACS+ . Si votre périphérique réseau prend en charge RADIUS et/ou TACACS+, ISE peut le prendre en charge !

Il existe de nombreuses raisons pour lesquelles les périphériques Cisco et non Cisco ne sont pas répertoriés :

- Notre équipe d'assurance qualité ne peut pas se permettre de tester chaque combinaison matérielle et logicielle avec chaque version ISE.
- **Les nouvelles plates-formes matérielles** doivent être acquises et testées, ce qui se produit généralement dans les 6 à 9 mois suivant la sortie du matériel.
- **Chaque modèle d'une famille de matériels** n'est pas validé : un modèle est choisi, puis utilisé pour représenter la famille de matériels.
- **Chaque version logicielle** n'est pas validée : une version logicielle de plate-forme publiée recommandée par l'équipe de la plate-forme est choisie, quelques mois avant la version ISE réelle pour la planification de la validation QA.
- Les anciennes versions ISE ne sont pas testées avec un nouveau logiciel Network Device, mais elles doivent toujours être conformes aux normes.

Ce que vous pouvez faire exactement avec ISE est ensuite déterminé par les capacités matérielles et logicielles de votre périphérique réseau. Il est toujours recommandé d'essayer le matériel et les logiciels de votre périphérique réseau dans votre laboratoire avec ISE avant de le déployer en production afin de vous assurer qu'il se comporte comme prévu.

Profils NAD (Network Access Device) ISE

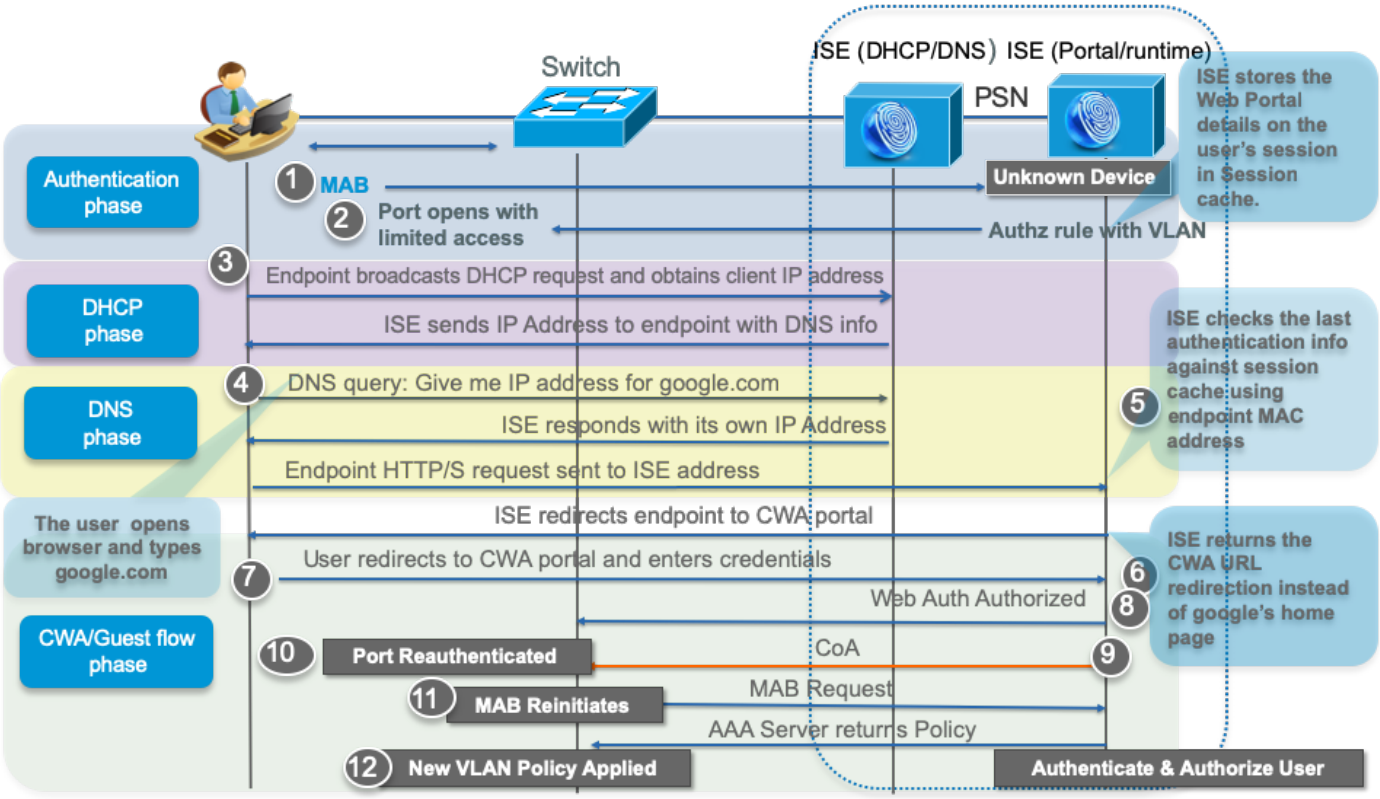
Si vous avez :

- matériel non Cisco
- matériel de périphérique réseau bas de gamme peu coûteux
- matériel de périphérique réseau plus ancien
- Logiciel de périphérique réseau plus ancien

vous pouvez ensuite utiliser nos profils et configurations NAD tiers ISE ou créer votre propre profil NAD personnalisé. À l'aide d'un profil NAD, vous pouvez entièrement personnaliser la manière dont ISE communique avec votre périphérique réseau, que ce soit sur des ports personnalisés pour la CoA RADIUS ou si vous devez utiliser des VLAN d'authentification au lieu de la redirection d'URL.

Prise en charge VLAN d'authentification

Si vous disposez d'anciens commutateurs hérités incapables de la norme 802.1X, ISE peut contrôler les terminaux à l'aide de VLAN d'authentification. Il s'agit d'une méthode de contrôle très rudimentaire qui utilise DNS et DHCP pour rediriger le trafic HTTP vers un portail Web où l'utilisateur peut s'authentifier. Pour plus d'informations, reportez-vous à Prise en charge des périphériques réseau tiers dans Cisco ISE dans les Guides des administrateurs ISE.



Problèmes liés à l'utilisation des VLAN d'authentification

- Vous ne pouvez pas contrôler plusieurs périphériques par port.
- Le filtrage du trafic est très rudimentaire avec les VLAN de couche 2 - pas de contrôle IP/protocole/port de couche 3/4 sauf avec une VACL ou VRF.
- Aucune segmentation Est/Ouest au sein d'un VLAN ne signifie que les programmes malveillants sont facilement propagés à d'autres points d'extrémité au sein des VLAN, qu'ils soient non fiables ou fiables.