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

Table des matières

Introduction

- ISE prend en charge les protocoles RADIUS et TACACS

Guides de compatibilité ISE

- Fonctionnalités des périphériques réseau pour ISE
- Comment connaissez-vous les fonctionnalités de vos périphériques réseau ?
- Impossible de voir votre matériel ou vos logiciels dans le Guide de compatibilité ISE

Profils de périphérique d'accès réseau (NAD) ISE

Prise en charge VLAN d'authentification

- Problèmes d'utilisation des VLAN d'authentification

Introduction

Ce document décrit comment vérifier la compatibilité de Cisco Identity Services Engine (ISE) avec votre périphérique d'accès 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 standard RADIUS et TACACS, ISE peut le prendre en charge !

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

Les capacités d'un périphérique réseau donné à 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 MAC Authentication Bypass (MAB), RADIUS Change of Authorization (CoA) [RFC-5176], les listes de contrôle d'accès de couche 3/4 (ACL), les ACL basées sur le domaine, la redirection d'URL ou la 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 le rechercher avec le fournisseur ou l'équipe produit.

Quand les gens demandent ; ISE prend-il en charge mon périphérique réseau ? ISE peut-elle m'offrir toutes ces fonctionnalités modernes de contrôle d'accès, même avec ce commutateur ancien et peu coûteux ?

Pour ces commutateurs plus anciens et moins coûteux, ISE offre des fonctionnalités telles que SNMP CoA et Authentication VLAN pour fournir des fonctionnalités similaires nécessaires pour

gérer le flux Guest, BYOD et Posture.

Guides de compatibilité ISE

Consultez 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, attribution de VLAN, listes de contrôle d'accès téléchargeables
Profilage	RADIUS CoA et sondes de profilage
BYOD	RADIUS CoA, redirection d'URL + ID de session
Invité	RADIUS CoA, redirection d'URL + ID de session, authentification Web locale
URL d'origine invité	RADIUS CoA, redirection d'URL + ID de session, authentification Web locale
Posture	RADIUS CoA, redirection d'URL + ID de session
MDM	RADIUS CoA, redirection d'URL + ID de session
TrustSec	Classification SGT

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

Créez un profil de périphérique d'accès réseau (NAD).

Comment connaissez-vous les fonctionnalités de vos périphériques réseau ?

Les fonctionnalités des combinaisons matérielles et logicielles validées sont documentées dans nos guides de compatibilité ISE. Pour tous les autres, vous devez effectuer des recherches sur les sites Web des fournisseurs, la documentation produit, les forums, etc. Parfois, il vous suffit de jouer dans vos travaux pratiques pour découvrir 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 vos logiciels dans le Guide de compatibilité ISE

Le simple fait qu'un modèle matériel ou une version logicielle ne soit pas explicitement répertorié ne signifie pas qu'il ne fonctionnera pas, mais seulement que vous ne l'avez pas validé avec ISE ! La section Périphériques d'accès réseau pris en charge des Guides de compatibilité ISE indique que 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 au réseau (NAD) client Cisco ou non-Cisco RADIUS qui implémente un comportement RADIUS commun (similaire à Cisco IOS 12.x) pour l'authentification basée sur les normes.

ISE prend en charge des 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 peuvent ne pas être répertoriés :

- Notre équipe d'assurance qualité ne peut pas se permettre de tester chaque combinaison matérielle et logicielle avec chaque version ISE.
- De 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 sélectionné, puis il est utilisé pour représenter la famille de matériels.
- Chaque version logicielle n'est pas validée : une version logicielle recommandée par l'équipe de la plate-forme est sélectionnée quelques mois avant la version ISE pour la planification de la validation de l'assurance qualité.
- Les versions ISE plus anciennes ne sont pas testées avec des logiciels Network Device plus récents, mais elles doivent toujours être conformes aux normes.

Ce que vous pouvez faire 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 d'être sûr qu'il se comporte comme prévu.

Profils de périphérique d'accès réseau (NAD) ISE

Si vous avez :

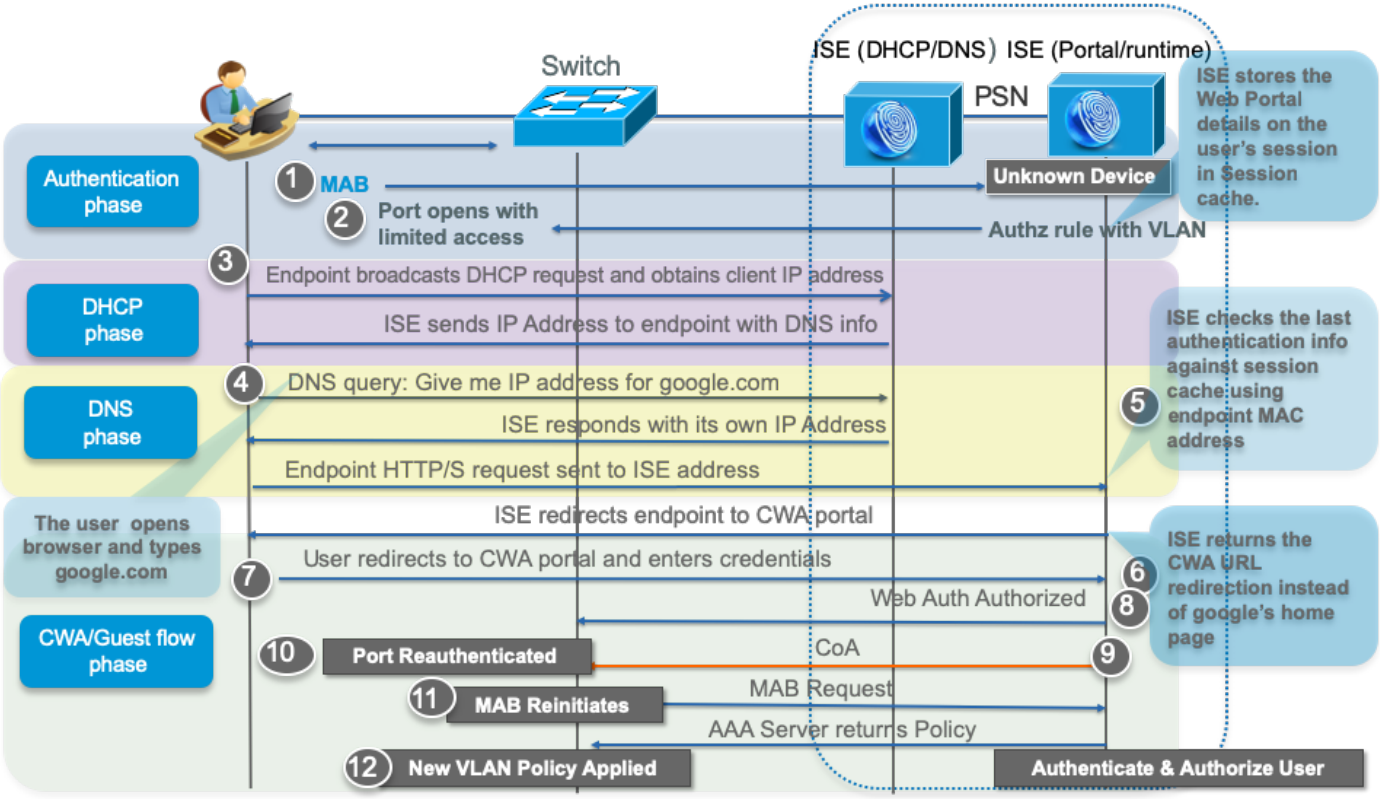
- matériel non-Cisco
- matériel de périphérique réseau bas de gamme et peu coûteux
- matériel de périphérique réseau plus ancien
- ancien logiciel de périphérique réseau

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 façon dont ISE communique avec votre périphérique réseau, que ce soit sur des ports personnalisés pour RADIUS CoA 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 qui ne sont pas compatibles avec 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 les protocoles 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 la section Third-Party Network Device Support in Cisco ISE dans les guides d'administration d'ISE.



Problèmes d'utilisation des VLAN d'authentification

- Vous ne pouvez pas contrôler plusieurs périphériques par port.
- Le filtrage du trafic est très rudimentaire avec les VLAN L2 : aucun contrôle IP/protocole/port L3/4, sauf avec une VACL ou un VRF.
- L'absence de segmentation Est/Ouest au sein d'un VLAN signifie que les programmes malveillants se propagent facilement à d'autres terminaux au sein des VLAN, qu'ils soient non fiables ou fiables.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.