ISE supporta il dispositivo di accesso alla rete?

Sommario

Introduzione

Questo documento descrive come verificare la compatibilità di Cisco Identity Services Engine (ISE) con il dispositivo di accesso alla rete (NAD).

ISE supporta i protocolli RADIUS e TACACS

Se il dispositivo di rete è in grado di inviare richieste di controllo dell'accesso utilizzando i protocolli standard RADIUS e TACACS, ISE potrà supportarle!

ISE supporta RADIUS per eseguire il controllo degli accessi con tutti i meccanismi di imposizione supportati dall'hardware e dal software del dispositivo di rete.

Le funzionalità di un determinato dispositivo di rete per il controllo degli accessi basato sulle porte con lo standard IEEE 802.1X sono software e spesso dipendenti dall'hardware. Supportare solo RADIUS non significa che il dispositivo di rete supporti molte utili funzionalità di imposizione, come MAC Authentication Bypass (MAB), RADIUS Change of Authorization (CoA) [RFC-5176], Layer-3/4 Access Control Lists (ACL), ACL basati su dominio, reindirizzamento URL o segmentazione definita dal software con Cisco TrustSec. Non è sempre possibile stabilire la capacità di un determinato dispositivo di rete e potrebbe essere necessario eseguire una ricerca in merito con il fornitore o il team del prodotto.

Quando la gente lo chiede; ISE supporta il dispositivo di rete? In altre parole, ISE è in grado di offrirmi tutte queste moderne funzionalità di controllo degli accessi anche con questo vecchio ed economico switch?

Per questi switch più vecchi e meno costosi, ISE offre funzionalità come SNMP CoA e Authentication VLAN per fornire alcune funzionalità simili necessarie a gestire il flusso guest, BYOD e postura.

Guide alla compatibilità ISE

Controlla sempre le **Guide** alla **compatibilità ISE** per vedere cosa ha convalidato il nostro team QA

per ogni versione ISE.

Funzionalità dispositivi di rete per ISE

Si tratta delle funzionalità dei dispositivi di rete moderne normalmente richieste per offrire le funzionalità ISE:

Capacità ISE	Caratteristiche dispositivo di rete
AAA	802.1X, MAB, assegnazione VLAN, ACL scaricabili
Creazione profilo	Sonde di profilatura e CoA RADIUS
BYOD	RADIUS CoA, reindirizzamento URL + SessionID
Guest	RADIUS CoA, reindirizzamento URL + ID sessione, autenticazione Web locale
URL di origine guest	RADIUS CoA, reindirizzamento URL + ID sessione, autenticazione Web locale
Postura	RADIUS CoA, reindirizzamento URL + SessionID
MDM	RADIUS CoA, reindirizzamento URL + SessionID
TrustSec	Classificazione SGT

Cosa fare se il dispositivo di rete non dispone di tutte le caratteristiche per la funzionalità ISE?

Creare un profilo NAD (Network Access Device).

Come si conoscono le funzionalità dei dispositivi di rete?

Le funzionalità per le combinazioni convalidate di hardware e software sono facilmente documentate nelle Guide alla compatibilità ISE. Per tutti gli altri, è necessario eseguire ricerche su siti Web dei fornitori, documentazione dei prodotti, forum, ecc. A volte può essere sufficiente giocare in laboratorio per scoprire cosa funziona e cosa no e creare un profilo di dispositivo di rete per le diverse combinazioni di funzionalità.

Impossibile visualizzare l'hardware o il software nella Guida alla compatibilità ISE

Il fatto che un modello hardware o una versione software non siano esplicitamente elencati non significa che non funzioneranno; è solo che non è stato convalidato con ISE. Nella sezione **Dispositivi di accesso alla rete supportati** delle Guide alla compatibilità ISE viene indicato che ISE supporta RADIUS, indipendentemente dal fornitore o dal modello:

> Cisco ISE supporta l'interoperabilità con qualsiasi dispositivo NAD (Client Network Access Device) Cisco Cisco RADIUS che implementa il comportamento RADIUS comune (simile a Cisco IOS 12.x) per l'autenticazione basata su standard.

ISE supporta standard di protocollo come RADIUS, gli standard RFC associati, e TACACS+ . Se il dispositivo di rete supporta RADIUS e/o TACACS+, ISE può supportarlo!

I dispositivi Cisco e non Cisco potrebbero non essere elencati per diversi motivi:

- Il nostro team di controllo della qualità non può permettersi di testare ogni singola combinazione hardware e software con ogni versione ISE.
- **Le nuove piattaforme hardware** devono essere acquisite e testate, in genere entro 6-9 mesi dalla release dell'hardware.
- **Ogni modello di una famiglia di hardware** non viene convalidato. Un modello viene scelto e quindi utilizzato per rappresentare la famiglia di hardware.

- **Ogni versione del software** non viene convalidata - viene scelta una versione del software della piattaforma rilasciata consigliata dal team della piattaforma, pochi mesi prima dell'effettiva versione ISE per la pianificazione della convalida del controllo qualità.
- Le versioni precedenti di ISE non sono testate con i nuovi software per dispositivi di rete, ma devono essere conformi agli standard.

Ciò che puoi fare con ISE è determinato dalle funzionalità hardware e software del tuo dispositivo di rete. Si consiglia sempre di provare l'hardware e il software del dispositivo di rete in laboratorio con ISE prima di distribuirlo alla produzione, in modo da avere la certezza che funzioni come previsto.

Profili NAD (Network Access Device) ISE

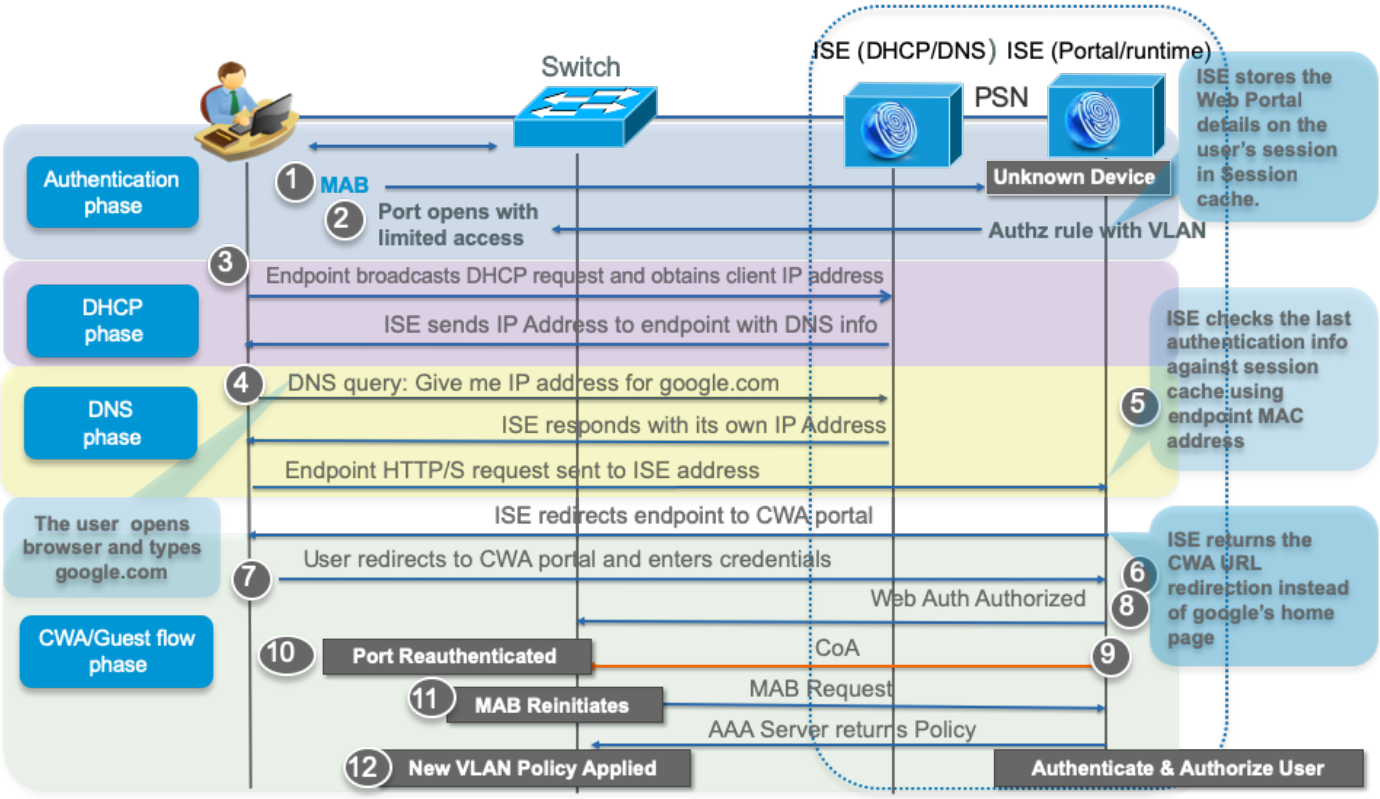
Se si dispone di:

- hardware non Cisco
- hardware per dispositivi di rete low-end a basso costo
- hardware per dispositivi di rete meno recenti
- software per dispositivi di rete meno recenti

quindi puoi usare i nostri profili e configurazioni ISE di terze parti o creare il tuo profilo NAD personalizzato. Usando un profilo NAD, è possibile personalizzare completamente la comunicazione di ISE con il dispositivo di rete, sia che si trovi sulle porte personalizzate di RADIUS CoA o che si desideri usare le VLAN di autenticazione anziché il reindirizzamento dell'URL.

Supporto VLAN di autenticazione

Se si usano alcuni switch legacy non compatibili con 802.1X, ISE può controllare l'endpoint con VLAN di autenticazione. Si tratta di un metodo di controllo molto approssimativo che utilizza DNS e DHCP per reindirizzare il traffico HTTP a un portale Web in cui l'utente può eseguire l'autenticazione. Per ulteriori informazioni, vedere il supporto di dispositivi di rete di terze parti in Cisco ISE nel manuale ISE Administrators Guide.



Problemi nell'utilizzo delle VLAN di autenticazione

- Non è possibile controllare più dispositivi per porta.
- Il filtro del traffico è molto rozzo con le VLAN L2 - senza controllo protocollo/porta L3/4 IP tranne che con un VACL o VRF.
- L'assenza di segmentazione est/ovest all'interno di una VLAN significa che il malware si diffonde facilmente ad altri endpoint all'interno delle VLAN, siano essi non attendibili o attendibili.