SSE Do Not Decrypt voor IPS en SWG Decryption Bypass configureren

Inhoud

uitgifte

HTTPS-verkeer naar bestemmingen in de financieringscategorie blijft een Cisco SSE-certificaat presenteren in plaats van het oorsprongscertificaat van de website, zelfs na het toevoegen van de Finance-categorie of specifieke domeinen aan een Do Not Decrypt (DND) -lijst en het toepassen van de relevante toegangsregel. Dit gedrag wordt waargenomen bij de toegang tot sites via de Zero Trust Access Client (TIA), met name van invloed op de toegang tot aan financiën gerelateerde websites zoals https://onlinesbi.sbi.bank.in/ waar end-to-end-certificaatzichtbaarheid vereist is.

Het verwachte gedrag is dat wanneer een site of inhoudscategorie aan de DND-lijst wordt toegevoegd, het oorsprongscertificaat van de website aan de browser kan worden gepresenteerd in plaats van het Cisco SSE-certificaat. Het Cisco SSE-certificaat blijft echter worden gepresenteerd, wat aangeeft dat verkeersdecodering nog steeds plaatsvindt ondanks de DND-configuratie.

milieu

- Cisco Secure Service Edge (SSE)
- Zero Trust Access Client (TIA)-connectiviteit
- Globale IPS-decodering ingeschakeld
- IPS actief op toegangsbeleid
- Financieringscategorie geconfigureerd in de lijst Niet decoderen binnen het beveiligingsprofiel
- Toegangsregels toegepast met bijbehorende beveiligingsprofielen

resolutie

De resolutie houdt in dat u begrijpt dat Cisco SSE twee verschillende soorten decodering uitvoert en de juiste instellingen voor niet-decoderen voor beide decoderingstypen configureert.

SSE-decoderingstypen begrijpen

Cisco SSE voert twee afzonderlijke decoderingsprocessen uit:

- SWG (Secure Web Gateway)-decryptie - webproxydecryptie
- IPS-decodering - Intrusion Prevention System-decodering

Niet ontsleutelen items geconfigureerd in een beveiligingsprofiel zijn alleen van toepassing op SWG decryptie en niet voorkomen dat IPS decryptie. Wanneer algemene IPS-decodering is ingeschakeld en IPS actief is op elk toegangsbeleid, vindt nog steeds IPS-decodering plaats, waardoor het Cisco SSE-certificaat aan de browser wordt gepresenteerd.

Configuratiestappen

Stap 1: Voeg sites of inhoudscategorieën toe aan de lijst Niet decoderen.

De lijst Systeemvoorziening Niet decoderen wordt toegepast op alle IPS-profielen. Het toevoegen van een site of inhoudscategorie aan deze lijst Systeemvoorziening resulteert in de presentatie van het oorsprongscertificaat van de website, waardoor IPS-decryptie effectief wordt omzeild.

Stap 2: Controleer of er geen aanvullende beleidswijzigingen nodig zijn.

Het is niet nodig om te verwijzen naar de lijst Systeemvoorziening Niet decoderen binnen het toegangsbeleid. De lijst wordt automatisch toegepast op alle IPS-profielen.

validatietests

Deze validatiemethoden kunnen worden gebruikt om de juiste configuratie te bevestigen:

Methode 1: Domeinnaam toevoegen aan opgegeven systeem Lijst niet decoderen

Als u het specifieke domein toevoegt aan de lijst Systeemvoorziening Niet decoderen, kan het certificaat van de website van oorsprong worden gepresenteerd in plaats van het Cisco SSE-certificaat.

Methode 2: Wereldwijde IPS-decodering tijdelijk uitschakelen (alleen voor testen)

Het tijdelijk uitschakelen van wereldwijde IPS-decryptie zorgt er ook voor dat het oorsprongscertificaat wordt gezien voor de geteste site, wat bevestigt dat IPS-decryptie de oorzaak was van de Cisco SSE-certificaatpresentatie.

Verwachte resultaten

Na de juiste configuratie:

- Sites of inhoudscategorieën die zijn toegevoegd aan de lijst Systeemvoorziening Niet ontcijferen presenteren hun oorsprongscertificaten.
- Zowel SWG- als IPS-decodering worden omzeild voor de opgegeven sites of categorieën.
- In de browser wordt het eigenlijke websitecertificaat weergegeven in plaats van het Cisco SSE-certificaat.

Oorzaak

Het probleem doet zich voor omdat Cisco SSE twee verschillende decryptieprocessen uitvoert: SWG-decryptie en IPS-decryptie. Ontcijfert geen items die zijn geconfigureerd binnen beveiligingsprofielen en omzeilt SWG-decodering alleen. Wanneer algemene IPS-decodering is ingeschakeld en IPS actief is op toegangsbeleid, blijft IPS-decodering onafhankelijk plaatsvinden, waardoor het Cisco SSE-certificaat aan de browser wordt gepresenteerd, zelfs wanneer sites zijn opgenomen in DND-lijsten met beveiligingsprofielen.

Om beide soorten decryptie volledig te omzeilen, moeten sites of inhoudscategorieën worden toegevoegd aan de lijst Systeemvoorziening Niet decoderen, die van toepassing is op alle IPS-profielen en voorkomt dat zowel SWG- als IPS-decryptie optreedt.

Gerelateerde inhoud

- Effectieve niet-ontsleutelingslijst maken voor beveiligde toegang
- Problemen oplossen en basisinformatie verzamelen voor beveiligde toegang
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.