Stappen voor de integratie van Cisco Email Threat Defense (ETD) met Cisco Secure Access:

Inhoud

Inleiding

Dit document illustreert de stappen voor de integratie van Cisco Email Threat Defense (ETD) met Cisco Secure Access (SA) voor e-mail DLP in ETD SMTP Inline Mode. Dit zorgt ervoor dat alle uitgaande e-mails die via ETD worden verzonden, worden gescand op DLP met behulp van Cisco Secure Access (SA).

Overzicht

In de huidige gedistribueerde werkomgeving blijft e-mail het belangrijkste communicatiemiddel voor bedrijven en daarmee het meest voorkomende doelwit voor cyberaanvallen en data-exfiltratie. Om deze evoluerende uitdagingen aan te pakken, biedt Cisco een uitgebreide aanpak voor e-mailbeveiliging via Email Threat Defense (ETD) en Secure Access Email Data Loss Prevention (DLP).

Door de mogelijkheden voor dreigingsdetectie van Cisco Email Threat Defense te combineren met de robuuste gegevensbescherming van Secure Access Email DLP, kunnen organisaties een verdedigingsstrategie met meerdere lagen opzetten. Deze aanpak beveiligt niet alleen de inbox van externe actoren, maar zorgt er ook voor dat gevoelige bedrijfsgegevens onder strikte controle

blijven, ongeacht waar de gebruiker zich bevindt of hoe ze toegang krijgen tot hun e-mail.

Voorwaarden

Toegang tot onderstaande console.

1. Cisco Email Threat Defense Console (ETD) in de inline modus.

   De ETD-console fungeert als het centrale beheervlak voor uw e-mailbeveiligingshouding. Toegang tot deze console is de eerste stap in het configureren van uw omgeving om u te beschermen tegen geavanceerde bedreigingen.

   - Waarom "Inline Mode" belangrijk is: Wanneer ETD is geconfigureerd in Inline Mode, fungeert het als een mail transfer agent (MTA) of een directe integratie die in het pad van de e-mailstroom zit. Hierdoor kan het systeem berichten inspecteren, blokkeren of wijzigen voordat ze in de inbox van de ontvanger worden afgeleverd.
2. Cisco Secure Access Console (SA)

Cisco Secure Access is het uniforme, in de cloud geleverde beveiligingsplatform dat verschillende beveiligingsservices, waaronder Data Loss Prevention (DLP), integreert in één samenhangende architectuur.

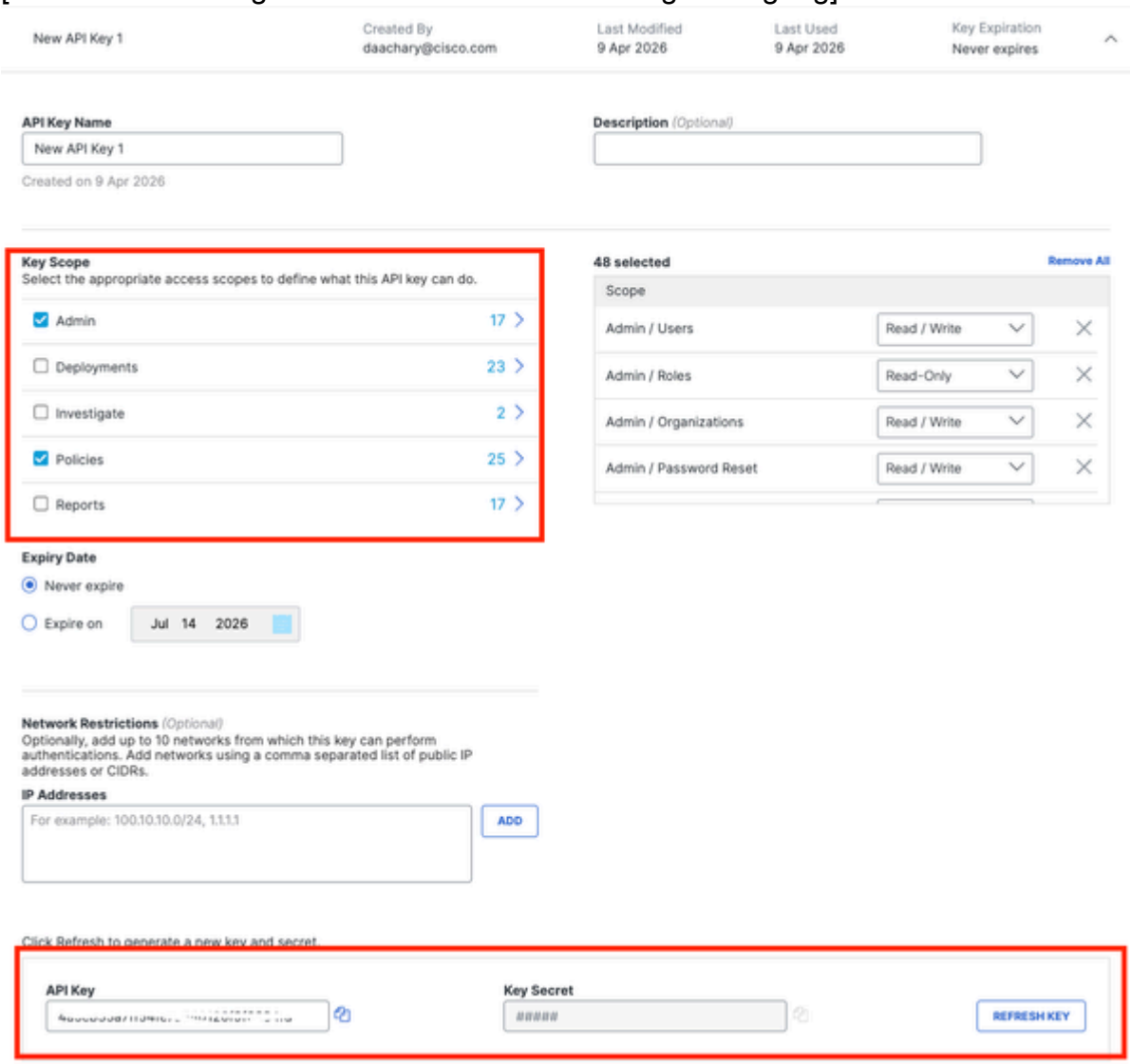
- Waarom de SA-console vereist is: De Secure Access-console is de orkestratie-hub voor het beveiligingsbeleid van uw organisatie. Terwijl ETD de dreigingsspecifieke e-mailstroom afhandelt, definieert u in de Secure Access-console het bredere DLP-beleid dat bepaalt hoe gevoelige gegevens worden geïdentificeerd en behandeld in uw hele onderneming.
- Consolerol: met deze console kunnen beheerders regels voor gegevensclassificatie maken en toepassen (bijvoorbeeld PII, creditcardnummers of interne projectcodes identificeren). Door toegang te krijgen tot de SA-console, kunt u ervoor zorgen dat uw DLP-beleid voor e-mail wordt gesynchroniseerd met uw algemene beveiligingsstrategie, waardoor consistente handhaving van zowel e-mailverkeer mogelijk is.

Configureren

Integratiestappen

Stap 1: API-referenties genereren in Cisco Secure Access

Om te beginnen moet u de benodigde API-referenties genereren in de Secure Access-console om de verbinding te autoriseren.

1. Log in op het Cisco Secure Access-dashboard.
2. Navigeer naar Admin>API-sleutels.
3. Selecteer de optie om een nieuwe API-sleutel te maken.
4. Wijs de volgende scopes toe aan de sleutel: AdminandPolicy.
    - [Screenshot: Configuratie API-sleutel voor beveiligde toegang]
    - 

Stap 2: Vervaldatum van sleutel configureren

Bepaal de levenscyclus van uw API-sleutel op basis van het beveiligingsbeleid van uw organisatie.

- Optie 1: Nooit verlopen – Biedt ononderbroken service zonder handmatige rotatie.
- Optie 2: Specifieke datum: stelt een gedefinieerde vervaldatum in.

- Belangrijke opmerking: als u een vervaldatum wilt instellen, moet u een rotatieproces plannen. U moet de API-sleutels in de ETD-console vóór de vervaldatum opnieuw configureren om een onderbreking van uw DLP-services te voorkomen.

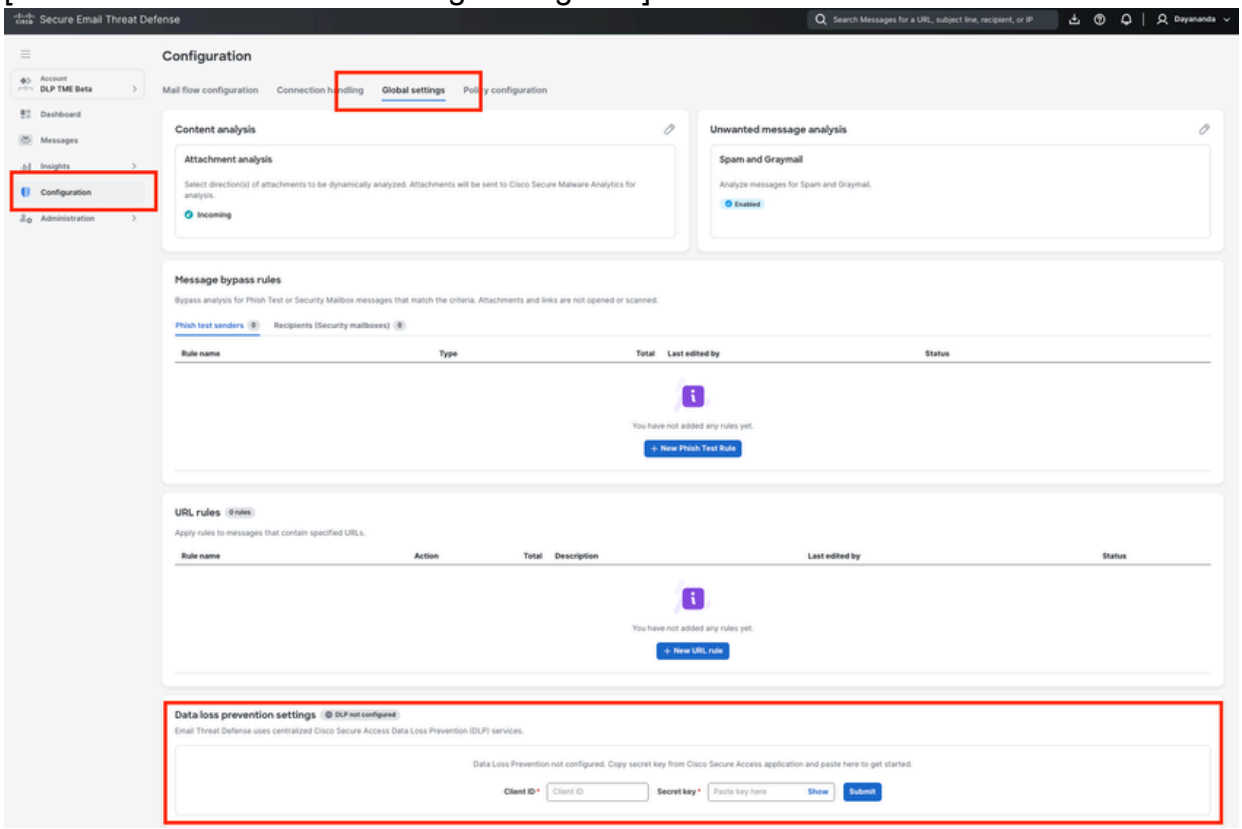
Stap 3: Beveilig uw referenties

Zodra de sleutel is gegenereerd, geeft het systeem de API-sleutel en Key Secret weer.

- Actie: Kopieer en bewaar deze referenties op een veilige locatie (bijvoorbeeld een wachtwoordbeheerder).
- Waarschuwing: Het sleutelgeheim is niet zichtbaar nadat u van dit scherm bent weggegaan. Als u verloren bent, moet u een nieuw sleutelpaar genereren.

Stap 4: Toegang tot de ETD-configuratie

Als uw referenties zijn beveiligd, gaat u naar de ETD-console om de koppeling te voltooien.

1. Log in op de Cisco ETDconsole.
2. Navigeer naar Configuration>Globale instellingen.
    - [Screenshot: ETD Global Settings Navigation]
    -


Stap 5: Integratie voltooien

Voltooi de handshake door de referenties in te voeren die zijn verkregen via Secure Access.

1. Zoek in het menu Algemene instellingen de sectie Gegevensverliespreventie (DLP).
2. Voer de client-ID (API-sleutel) en de geheime sleutel (Key Secret) in die u in stap 3 hebt opgeslagen.
3. Sla uw wijzigingen op.

Na succesvolle validatie is de integratie tussen Cisco ETD en Cisco Secure Access voltooid en is uw DLP-beleid klaar voor handhaving in uw e-mailverkeer.

Nu is de integratie van ETD en Secure Access voltooid.
OPMERKING: Raadpleeg "Een DLP-beleid voor e-mail configureren in Cisco Secure Access (SA) en Cisco Email Threat Defense (ETD)" om DLP-beleid te maken in Cisco Secure Access voor e-mail DLP.

Opmerkingen voor probleemoplossing

Als u problemen ondervindt tijdens of na het integratieproces, bekijkt u de volgende algemene scenario's en herstelstappen:

1. API-referenties niet geaccepteerd in ETD

- Symptoom: bij het invoeren van de client-ID en geheime sleutel in ETD, retourneert het systeem een verificatiefout.
- Resolutie:
  - Controleer of de API-sleutel is gemaakt met de exacte vereiste scopes: "Admin" en "Beleid". Als er andere scopes zijn geselecteerd of deze zijn gemist, mislukt de verbinding.
  - Zorg ervoor dat er geen spaties aan de voorzijde of achterzijde per ongeluk worden gekopieerd wanneer u de client-ID of geheime sleutel in de ETD-console plakt.

2. Verloren of vergeten sleutelgeheim

- Symptoom: U bent weggenavigeerd van het scherm Secure Access API maken en kunt de

Key Secret niet meer bekijken.
- Oplossing: om veiligheidsredenen wordt het Sleutelgeheim slechts eenmaal weergegeven op het moment van maken. Als u het niet veilig hebt opgeslagen, moet u de onvolledige API-sleutel in Secure Access verwijderen en een nieuwe genereren.

3. DLP-beleid wordt niet toegepast op e-mailverkeer

- Symptoom: de integratie wordt als succesvol weergegeven, maar het geconfigureerde DLP-beleid vangt of blokkeert geen gevoelige e-mails.
- Resolutie:
  - Controleer de vervaldatum van de API: Als u "Selecteer een specifieke datum" hebt geselecteerd voor het vervallen van de API-sleutel (stap 2), controleert u of de sleutel niet is verlopen. Als dit het geval is, moet u een nieuw sleutelpaar genereren en toepassen.
  - ETD-implementatiemodus verifiëren: Zorg ervoor dat Cisco ETD wordt geïmplementeerd in de inline-modus. ETD moet zich in het directe-mailstroompad bevinden om berichten actief te blokkeren of te wijzigen op basis van DLP-oordelen voor beveiligde toegang.
  - Synchronisatietijd: na de eerste integratie kunt u de back-endsystemen enkele minuten de tijd geven om het beleid te synchroniseren voordat u de DLP-regels test.

4. Verstoring van de service na een periode van stabiliteit

- Symptoom: DLP-handhaving stopt plotseling nadat het maandenlang correct heeft gefunctioneerd.
- Resolutie: dit wordt meestal veroorzaakt door een verlopen API-sleutel. Navigeer naar Admin -> API-sleutels in Cisco Secure Access om de status van de sleutel te controleren die voor ETD wordt gebruikt. Implementeer een belangrijk rotatieproces om de referenties in ETD bij te werken voordat de vervaldatum is bereikt.

Samenvatting

Het integreren van Cisco Email Threat Defense (ETD) met Cisco Secure Access (SA) is een cruciale stap in het vaststellen van een uniforme strategie voor het voorkomen van gegevensverlies (DLP). Door een beveiligde API-sleutel te genereren met "Admin"- en "Policy"-scopes in de Secure Access-console en deze referenties te configureren binnen de Global Settings van ETD, creëren beheerders een naadloze communicatiebrug tussen de twee platforms.

Zodra deze handshake is voltooid, kan ETD actief e-mailmetadata afgeven aan de Secure Access DLP-engine. Hierdoor kan uw organisatie al het gegevensbeschermingsbeleid beheren vanuit één gecentraliseerd dashboard (Secure Access) en tegelijkertijd een goede zichtbaarheid en handhaving van uw e-mailverkeer (ETD) behouden.

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.