Étapes d'intégration de Cisco Email Threat Defense (ETD) avec Cisco Secure Access :

Table des matières

Introduction

Ce document illustre les étapes d'intégration de Cisco Email Threat Defense (ETD) avec Cisco Secure Access (SA) pour Email DLP en mode ETD SMTP Inline. Cela garantit que tous les e-mails sortants transitant par ETD seront analysés à la recherche de DLP avec l'aide de Cisco Secure Access(SA).

Aperçu

Dans l'environnement de travail distribué d'aujourd'hui, la messagerie électronique reste le principal outil de communication des entreprises et, par conséquent, la cible la plus fréquente des cyberattaques et de l'exfiltration de données. Pour faire face à ces défis en constante évolution, Cisco propose une approche complète de la sécurité de la messagerie via Email Threat Defense (ETD) et Secure Access Email Data Loss Prevention (DLP).

En combinant les fonctionnalités de détection des menaces de Cisco Email Threat Defense avec la protection robuste des données de Secure Access Email DLP, les entreprises peuvent établir une stratégie de défense multicouche. Cette approche permet non seulement de sécuriser la boîte de réception contre les acteurs externes, mais également de garantir que les données sensibles

de l'entreprise restent strictement contrôlées, quel que soit l'emplacement de l'utilisateur ou la manière dont il accède à sa messagerie.

Conditions préalables

Accès à sous la console.

1. Cisco Email Threat Defense Console (ETD) en mode Inline.

   La console ETD sert de plan de gestion centralisé pour la sécurité de votre messagerie électronique. L'accès à cette console est la première étape de la configuration de votre environnement pour vous défendre contre les menaces avancées.

   - Pourquoi le « mode en ligne » est important :Lorsque ETD est configuré en mode en ligne, il agit comme un agent de transfert de courrier (MTA) ou une intégration directe qui se trouve sur le chemin du flux de courrier électronique. Cela permet au système d'inspecter, de bloquer ou de modifier les messages avant qu'ils ne soient envoyés à la boîte de réception du destinataire.
2. Cisco Secure Access Console (SA)

Cisco Secure Access est la plate-forme de sécurité unifiée fournie dans le cloud qui intègre divers services de sécurité, y compris la prévention des pertes de données (DLP), dans une architecture unique et cohésive.

- Pourquoi la console SA est-elle requise :La console Secure Access est le concentrateur d'orchestration des stratégies de sécurité de votre entreprise. Tandis qu'ETD gère le flux d'e-mails spécifiques aux menaces, la console d'accès sécurisé vous permet de définir les politiques DLP plus larges qui régissent la manière dont les données sensibles sont identifiées et traitées dans votre entreprise.
- Rôle de console : cette console permet aux administrateurs de créer et d'appliquer des règles de classification des données (par exemple, l'identification des informations d'identification personnelle, des numéros de carte de crédit ou des codes de projet internes). En accédant à la console SA, vous pouvez vous assurer que vos stratégies DLP de messagerie sont synchronisées avec votre stratégie de sécurité globale, ce qui permet une application cohérente sur l'ensemble du trafic de messagerie.

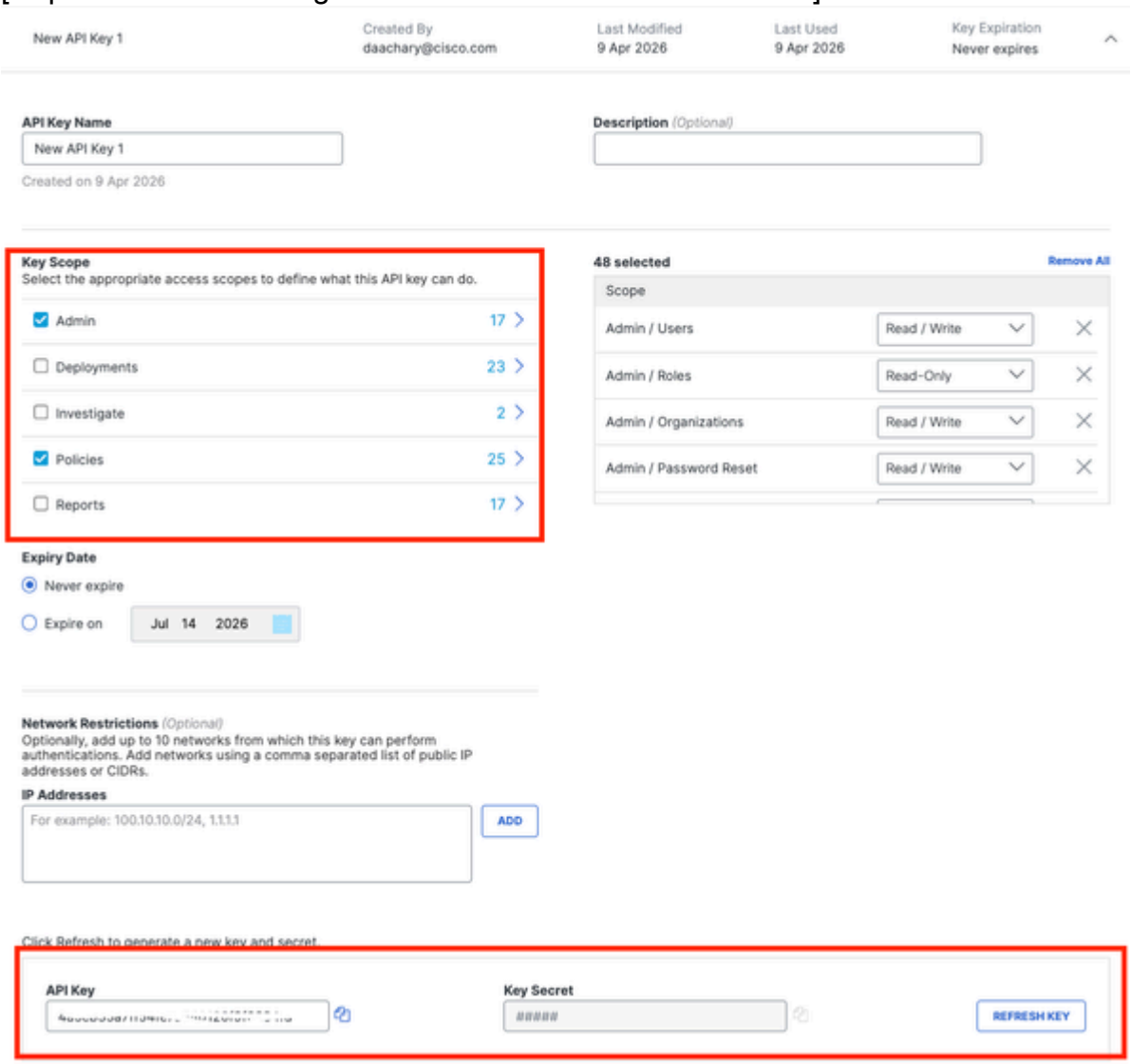
Configurer

Étapes d'intégration

Étape 1: Générer des identifiants API dans Cisco Secure Access

Pour commencer, vous devez générer les informations d'identification API nécessaires dans la console d'accès sécurisé pour autoriser la connexion.

1. Connectez-vous au tableau de bord Cisco Secure Access.
2. Accédez à Admin>Clés API.
3. Sélectionnez l'option permettant de créer une nouvelle clé API.
4. Attribuez les étendues suivantes à la clé :AdminandPolicy.
    - [Capture d’écran: Configuration de la clé API Secure Access]
    -



Étape 2: Configurer l'expiration des clés

Définissez le cycle de vie de votre clé API en fonction de la stratégie de sécurité de votre entreprise.

- Option 1: Never Expire : offre un service ininterrompu sans rotation manuelle.
- Option 2: Specific Date : définit un calendrier d'expiration défini.
    - Remarque importante : si vous choisissez de définir une date d'expiration, assurez-vous de planifier un processus de rotation. Vous devez reconfigurer les clés d'API dans la console ETD avant la date d'expiration pour éviter une interruption de vos services DLP.

Étape 3: Sécuriser vos informations d'identification

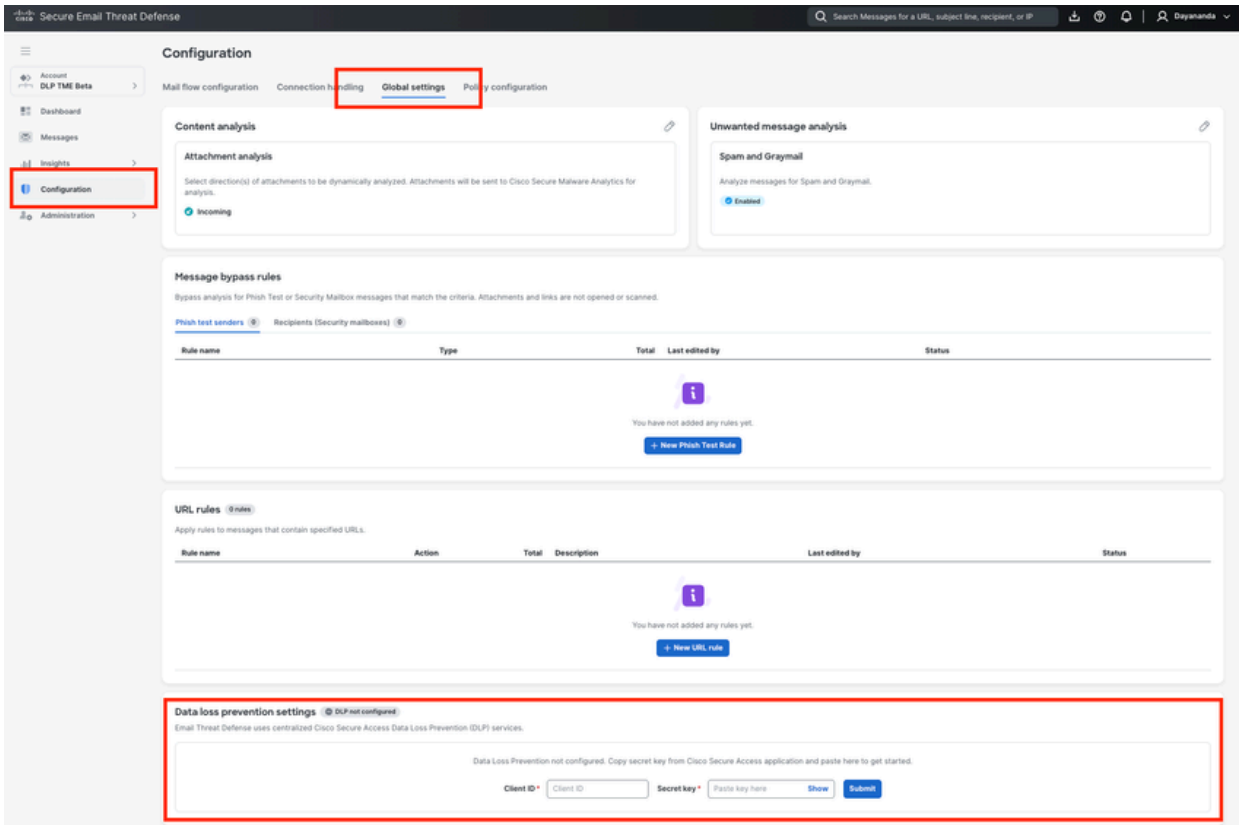
Une fois la clé générée, le système affiche la clé API et le secret de clé.

- Action : copiez et stockez ces informations d'identification dans un emplacement sécurisé (par exemple, un gestionnaire de mots de passe).
- Avertissement : Le secrétaire de touches ne sera pas visible lorsque vous vous serez éloigné de cet écran. En cas de perte, vous devrez générer une nouvelle paire de clés.

Étape 4: Accéder à la configuration ETD

Une fois vos informations d'identification sécurisées, passez à la console ETD pour finaliser la liaison.

1. Connectez-vous à la console Cisco ETD.
2. Accédez à Configuration>Global Settings.
    - [Capture d’écran: ETD [Navigation des paramètres généraux]

- 

Étape 5: Finaliser l'intégration

Terminez la connexion en entrant les informations d'identification obtenues à partir de Secure Access.

1. Dans le menu Paramètres globaux, localisez la section Prévention des pertes de données (DLP).
2. Entrez l'ID client(clé API) et la clé secrète(clé secrète) que vous avez enregistrés à l'étape 3.
3. Enregistrez vos modifications.

Une fois la validation réussie, l'intégration entre Cisco ETD et Cisco Secure Access est terminée et vos politiques DLP seront prêtes à être appliquées à l'ensemble de votre trafic de messagerie.

L'intégration de l'ETD et de l'accès sécurisé est désormais terminée.
NOTE: Reportez-vous à la section "Comment configurer une stratégie DLP de messagerie électronique dans Cisco Secure Access (SA) et Cisco Email Threat Defense (ETD)" pour créer une stratégie DLP dans Cisco Secure Access pour Email DLP.

Remarques de dépannage

Si vous rencontrez des problèmes pendant ou après le processus d'intégration, passez en revue les scénarios courants et les étapes de correction suivants :

1. Informations d'identification API non acceptées dans ETD

- Symptôme : lors de la saisie de l'ID client et de la clé secrète dans ETD, le système renvoie une erreur d'authentification.
- Résolution :
  - Vérifiez que la clé API a été créée avec les étendues exactes requises :« Admin » et« Policy ». Si d'autres étendues ont été sélectionnées ou si elles ont été manquées, la connexion échouera.
  - Assurez-vous qu'aucun espace de début ou de fin n'est copié accidentellement lors du collage de l'ID client ou de la clé secrète dans la console ETD.

2. Secret de clé perdu ou oublié

- Symptôme : vous vous êtes éloigné de l'écran de création de l'API Secure Access et vous ne pouvez plus afficher la clé secrète.
- Résolution : pour des raisons de sécurité, la clé secrète n'est affichée qu'une seule fois au moment de la création. Si vous ne l'avez pas enregistrée de manière sécurisée, vous devez supprimer la clé API incomplète dans Secure Access et en générer une nouvelle.

3. Les stratégies DLP ne s'appliquent pas au trafic de messagerie

- Symptôme : l'intégration est réussie, mais les stratégies DLP configurées n'interceptent pas ou ne bloquent pas les e-mails sensibles.
- Résolution :
  - Check API Expiration : si vous avez sélectionné « Select a specific date » (Sélectionner une date spécifique) pour l'expiration de la clé API (Étape 2), vérifiez que la clé n'a pas expiré. Si tel est le cas, vous devez générer et appliquer une nouvelle paire de clés.
  - Verify ETD Deployment Mode : vérifiez que Cisco ETD est déployé en mode Inline. ETD doit se trouver dans le chemin du flux de courrier direct pour bloquer ou modifier activement les messages en fonction des verdicts DLP d'accès sécurisé.
  - Temps de synchronisation : après l'intégration initiale, attendez quelques minutes que les systèmes principaux synchronisent les stratégies avant de tester les règles DLP.

4. Interruption du service après une période de stabilité

- Symptôme : l'application DLP cesse soudainement de fonctionner après avoir fonctionné correctement pendant des mois.
- Résolution : ceci est généralement dû à l'expiration d'une clé API. Accédez à Admin -> API

Keydans Cisco Secure Access pour vérifier l'état de la clé utilisée pour ETD. Mettez en oeuvre un processus de rotation des clés pour mettre à jour les informations d'identification dans ETDavant que la date d'expiration soit atteinte.

Résumé

L'intégration de Cisco Email Threat Defense (ETD) avec Cisco Secure Access (SA) est une étape essentielle dans l'établissement d'une stratégie unifiée de prévention des pertes de données (DLP). En générant une clé d'API sécurisée avec des étendues « Admin » et « Policy » dans la console d'accès sécurisé et en configurant ces informations d'identification dans les paramètres globaux d'ETD, les administrateurs créent un pont de communication transparent entre les deux plates-formes.

Une fois cette connexion terminée, ETD peut transférer activement les métadonnées de messagerie électronique au moteur DLP d'accès sécurisé. Cela permet à votre entreprise de gérer toutes les politiques de protection des données à partir d'un tableau de bord unique et centralisé (Secure Access) tout en conservant une visibilité et une application approfondies sur votre trafic de messagerie (ETD).

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.