Pasos para integrar Cisco Email Threat Defence (ETD) con Cisco Secure Access:

Contenido

Introducción

Este documento ilustra los pasos para integrar Cisco Email Threat Defence (ETD) con Cisco Secure Access (SA) para DLP de correo electrónico en modo en línea SMTP ETD. Esto garantiza que todos los correos electrónicos salientes que pasan a través de ETD se analizarán en busca de DLP con la ayuda de Cisco Secure Access (SA).

Overview

En el entorno de trabajo distribuido de hoy en día, el correo electrónico sigue siendo la principal herramienta de comunicación para las empresas y, en consecuencia, el objetivo más frecuente de los ciberataques y la fuga de datos. Para hacer frente a estos retos en constante evolución, Cisco ofrece un enfoque integral de la seguridad del correo electrónico mediante Email Threat Defence (ETD) y Secure Access Email Data Loss Prevention (DLP).

Al combinar las funciones de detección de amenazas de Cisco Email Threat Defence con la sólida protección de datos de DLP de correo electrónico de acceso seguro, las organizaciones pueden establecer una estrategia de defensa de varios niveles. Este enfoque no solo protege la bandeja de entrada de agentes externos, sino que también garantiza que los datos confidenciales de la

empresa permanezcan bajo un estricto control, independientemente de dónde se encuentre el usuario o de cómo acceda a su correo electrónico.

Prerequisites

Acceso a la consola inferior.

1. Cisco Email Threat Defence Console (ETD) en modo en línea.

   La consola de ETD sirve como el plano de gestión centralizada para su condición en materia de seguridad del correo electrónico. El acceso a esta consola es el primer paso en la configuración del entorno para defenderse frente a amenazas avanzadas.

   - Por qué es importante el "modo en línea":cuando ETD se configura en modo en línea, actúa como un agente de transferencia de correo (MTA) o una integración directa que se sitúa en la ruta del flujo de correo electrónico. Esto permite al sistema inspeccionar, bloquear o modificar mensajes antes de que se entreguen a la bandeja de entrada del destinatario.
2. Cisco Secure Access Console (SA)

Cisco Secure Access es la plataforma de seguridad unificada proporcionada a través de la nube que integra diversos servicios de seguridad, incluida la prevención de la pérdida de datos (DLP), en una única arquitectura cohesionada.

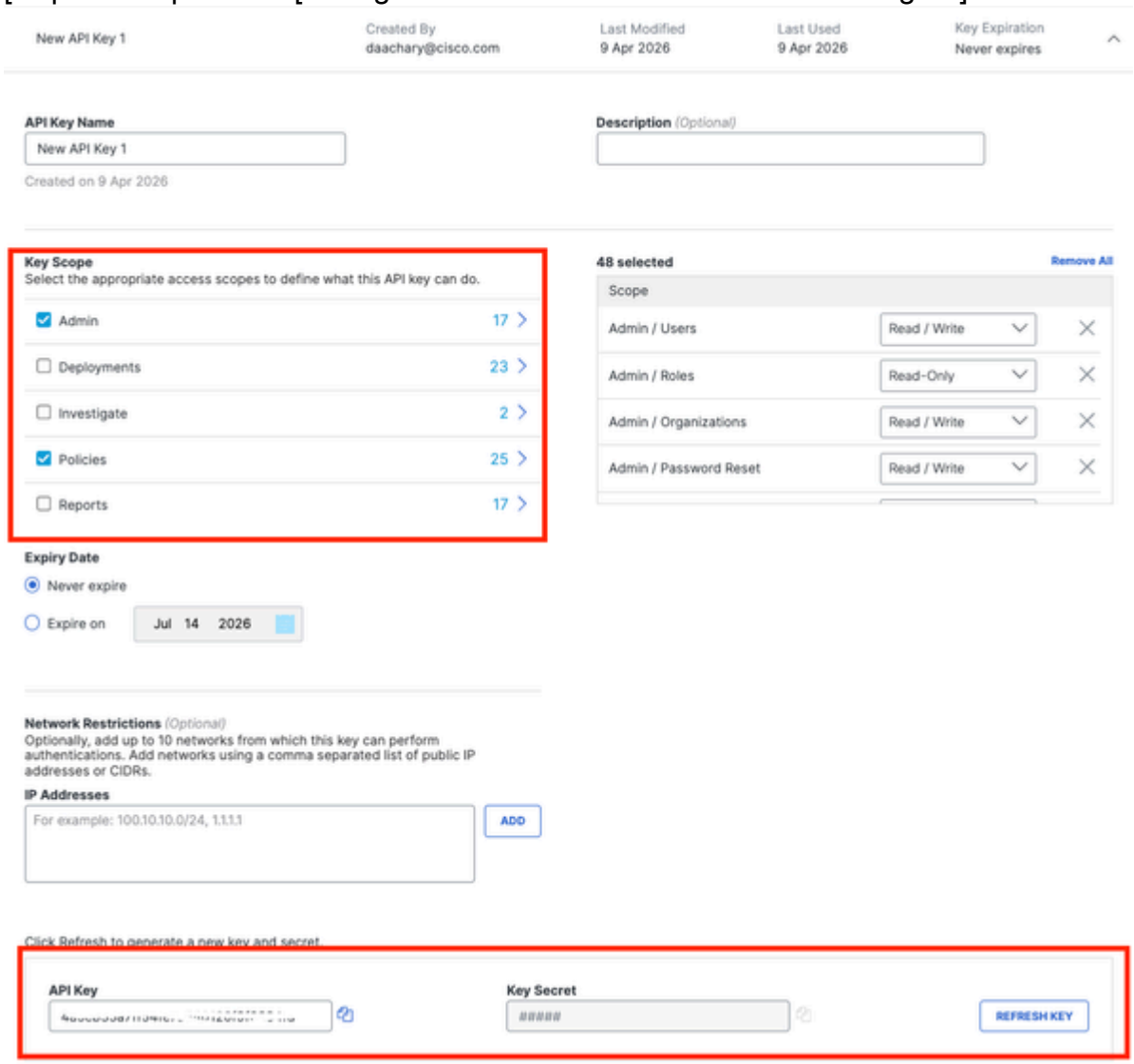
- Motivos por los que se requiere la consola de SA:La consola de Secure Access es el centro de orquestación de las políticas de seguridad de su organización. Mientras que ETD gestiona el flujo de correo electrónico específico de la amenaza, la consola de Secure Access es donde se definen las políticas de DLP más amplias que rigen la forma en que se identifican y gestionan los datos confidenciales en toda la empresa.
- Función de consola: esta consola permite a los administradores crear y aplicar reglas de clasificación de datos (por ejemplo, identificación de PII, números de tarjetas de crédito o códigos de proyecto internos). Al acceder a la consola de SA, puede garantizar que las políticas de DLP para correo electrónico están sincronizadas con su estrategia de seguridad general, lo que permite una aplicación uniforme en todo el tráfico de correo electrónico.

Configurar

Pasos de integración

Paso 1: Generación de credenciales de API en Cisco Secure Access

Para comenzar, debe generar las credenciales de API necesarias en la consola de Secure Access para autorizar la conexión.

1. Inicie sesión en el panel de acceso seguro de Cisco.
2. Vaya a Admin>Claves API.
3. Seleccione la opción para crear una nueva clave de API.
4. Asigne los ámbitos siguientes a la clave:AdminandPolicy.
    - [Captura de pantalla: [Configuración de clave de API de acceso seguro]
    - 

Paso 2: Configurar vencimiento de clave

Defina el ciclo de vida de la clave de la API en función de la política de seguridad de su organización.

- Opción 1: Never Expire (Nunca caduque): proporciona un servicio ininterrumpido sin rotación manual.
- Opción 2: Fecha específica: establece una línea de tiempo de vencimiento definida.
    - Nota Importante: Si decide establecer una fecha de vencimiento, asegúrese de planificar un proceso de rotación. Debe volver a configurar las claves API en la consola ETD antes de la fecha de vencimiento para evitar una interrupción en los servicios DLP.

Paso 3: Proteja sus credenciales

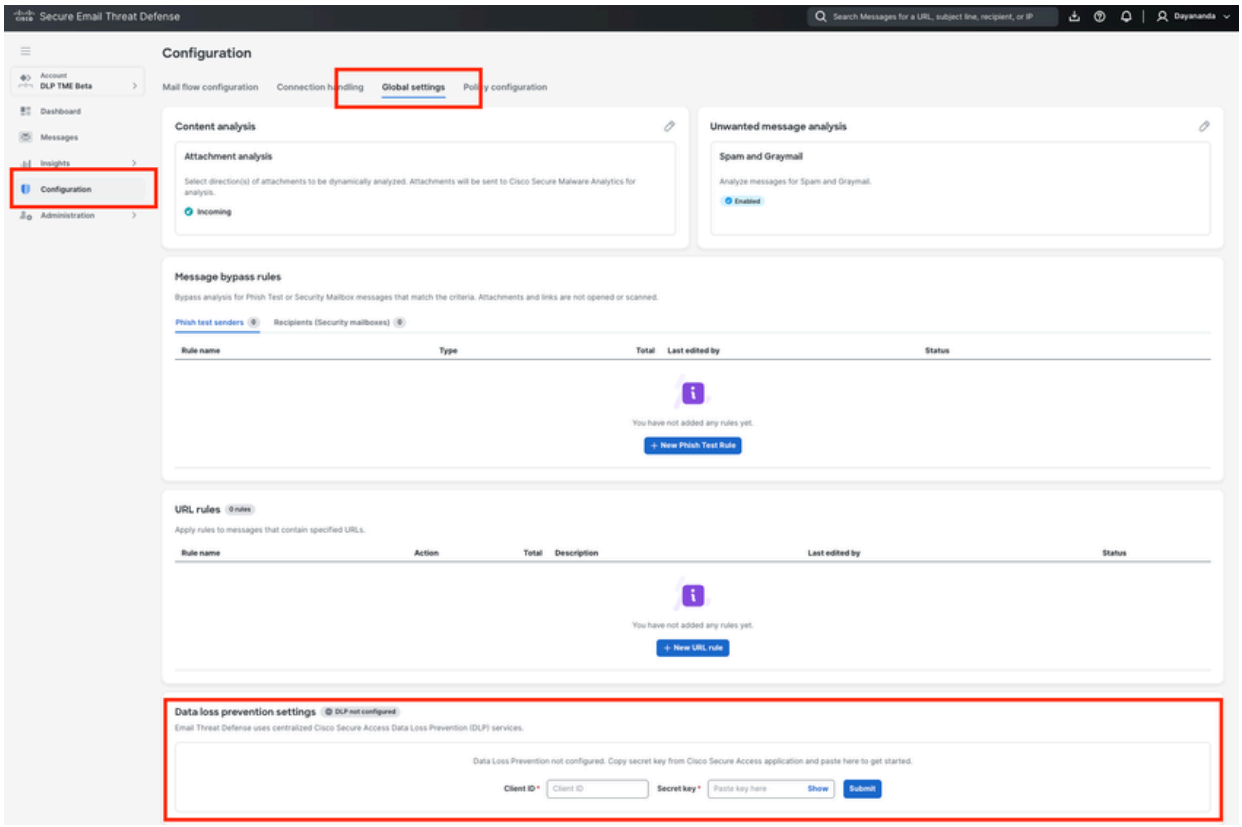
Una vez generada la clave, el sistema mostrará la clave API y la clave secreta.

- Acción:copie y almacene estas credenciales en una ubicación segura (por ejemplo, un administrador de contraseñas).
- Advertencia:ElSecreto de claves no estará visible después de salir de esta pantalla. Si se pierde, tendrá que generar un nuevo par de claves.

Paso 4: Acceso a la configuración de ETD

Con las credenciales protegidas, vaya a la consola de ETD para finalizar el enlace.

1. Inicie sesión en la consola Cisco ETD.
2. Vaya aConfiguración>Configuración global.
    - [Captura de pantalla: Configuración global de ETD [Navegación]

- 

Paso 5: Finalizar integración

Complete el protocolo de enlace introduciendo las credenciales obtenidas de Secure Access.

1. En el menúConfiguración global, localice la secciónPrevención de pérdida de datos (DLP).
2. Introduzca la ID del cliente (clave API) y la clave secreta (clave secreta) que guardó en el paso 3.
3. Guarde los cambios.

Una vez validada correctamente, la integración entre Cisco ETD y Cisco Secure Access ha finalizado y sus políticas de DLP estarán listas para su aplicación en todo el tráfico de correo electrónico.

Ahora se ha completado la integración de ETD y Secure Access.
NOTE: Consulte "Cómo configurar una política de DLP para correo electrónico en Cisco Secure Access (SA) y Cisco Email Threat Defence (ETD)"para crear una política de DLP en Cisco Secure Access para DLP para correo electrónico.

Notas sobre la resolución de problemas

Si tiene problemas durante o después del proceso de integración, revise los siguientes escenarios y pasos de solución comunes:

1. Credenciales de API no aceptadas en ETD

- Síntoma:Al introducir la ID de cliente y la clave secreta en ETD, el sistema devuelve un error de autenticación.
- Resolución:
  - Compruebe que la clave de la API se creó con los ámbitos necesarios exactos:"Admin"y"Policy". Si se seleccionaron otros ámbitos o estos se perdieron, la conexión fallará.
  - Asegúrese de que no haya espacios iniciales o finales copiados accidentalmente al pegar el ID de cliente o la clave secreta en la consola ETD.

2. Clave secreta perdida u olvidada

- Síntoma:Se ha alejado de la pantalla de creación de la API de Secure Access y ya no puede ver la clave secreta.
- Resolución:Por motivos de seguridad, el secreto de clave solo se muestra una vez en el momento de la creación. Si no lo guardó de forma segura, debe eliminar la clave API incompleta en Secure Access y generar una nueva.

3. Las políticas de DLP no se aplican al tráfico de correo electrónico

- Síntoma: la integración se muestra como correcta, pero las políticas de DLP configuradas no detectan ni bloquean los correos electrónicos confidenciales.
- Resolución:
  - Comprobar vencimiento de API:Si ha seleccionado "Seleccionar una fecha específica" para el vencimiento de la clave de API (paso 2), compruebe que la clave no ha caducado. Si es así, debe generar y aplicar un nuevo par de claves.
  - Verificar el modo de implementación de ETD:Asegúrese de que Cisco ETD se implementa en modo en línea. ETD debe encontrarse en la ruta de flujo de correo directo para bloquear o modificar activamente los mensajes en función de los veredictos de DLP de Secure Access.
  - Tiempo de sincronización: tras la integración inicial, espere unos minutos para que los sistemas back-end sincronicen las políticas antes de probar las reglas DLP.

4. Interrupción del servicio después de un período de estabilidad

- Síntoma: La aplicación de DLP deja de funcionar repentinamente después de haber funcionado correctamente durante meses.
- Resolución:Esto se debe normalmente a una clave de API caducada. Navegue hasta Admin

-> API Keyen Cisco Secure Access para verificar el estado de la clave utilizada para ETD. Implemente un proceso de rotación de claves para actualizar las credenciales en ETDantes de que se alcance la fecha de vencimiento.

Summary

La integración de Cisco Email Threat Defence (ETD) con Cisco Secure Access (SA) es un paso fundamental para establecer una estrategia unificada de prevención de la pérdida de datos (DLP). Al generar una clave de API segura con ámbitos "Admin" y "Policy" en la consola de Secure Access y configurar esas credenciales en la configuración global de ETD, los administradores crean un puente de comunicación perfecto entre las dos plataformas.

Una vez finalizado este intercambio de señales, ETD puede transferir de forma activa los metadatos del correo electrónico al motor DLP de Secure Access. Esto permite a su organización gestionar todas las políticas de protección de datos desde un único panel centralizado (acceso seguro), a la vez que mantiene una gran visibilidad y aplicación del tráfico de correo electrónico (ETD).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).