Etapas para integrar o Cisco Email Threat Defense(ETD) com o Cisco Secure Access:

Contents

Introdução

Este documento ilustra as etapas para integrar o Cisco Email Threat Defense(ETD) com o Cisco Secure Access(SA) para DLP de e-mail no modo em linha SMTP ETD. Isso garante que todos os e-mails de saída que passam pelo ETD serão verificados quanto ao DLP com a ajuda do Cisco Secure Access(SA).

Overview

No ambiente de trabalho distribuído de hoje, o e-mail continua sendo a principal ferramenta de comunicação para as empresas e, consequentemente, o alvo mais frequente de ataques cibernéticos e extração de dados. Para lidar com esses desafios em evolução, a Cisco oferece uma abordagem abrangente à segurança de e-mail por meio do Email Threat Defense (ETD) e do Secure Access Email Data Loss Prevention (DLP).

Combinando os recursos de detecção de ameaças do Cisco Email Threat Defense com a proteção de dados robusta do Secure Access Email DLP, as empresas podem estabelecer uma estratégia de defesa em várias camadas. Essa abordagem não apenas protege a caixa de entrada de agentes externos, mas também garante que os dados corporativos confidenciais

permaneçam sob controle rigoroso, independentemente de onde o usuário esteja localizado ou de como ele acessa seus e-mails.

Pré-requisitos

Acesso ao console abaixo.

1. Cisco Email Threat Defense Console (ETD) no modo em linha.

   O console ETD serve como o plano de gerenciamento centralizado para sua postura de segurança de e-mail. Acessar este console é a primeira etapa na configuração do seu ambiente para se defender contra ameaças avançadas.

   - Por que o "Modo em linha" é importante:Quando o ETD é configurado no Modo em linha, ele atua como um agente de transferência de e-mail (MTA) ou uma integração direta que se situa no caminho do fluxo de e-mail. Isso permite que o sistema inspecione, bloqueie ou modifique mensagens antes que elas sejam entregues na caixa de entrada do destinatário.
2. Console de acesso seguro (SA) Cisco

O Cisco Secure Access é a plataforma de segurança unificada disponibilizada em nuvem que integra vários serviços de segurança, incluindo Prevenção de Perda de Dados (DLP), em uma única arquitetura coesa.

- Por que o Console SA é necessário:O console Secure Access é o hub de orquestração para as políticas de segurança da sua organização. Enquanto o ETD lida com o fluxo de e-mail específico da ameaça, o console Secure Access é onde você define as políticas mais amplasDLP que controlam como os dados confidenciais são identificados e tratados em toda a empresa.
- Função do console:este console permite que os administradores criem e apliquem regras de classificação de dados (por exemplo, identificando PII, números de cartão de crédito ou códigos internos do projeto). Ao acessar o console do SA, você pode garantir que suas políticas de DLP de e-mail estejam sincronizadas com sua estratégia de segurança geral, permitindo a aplicação consistente em ambos os tráfegos de e-mail.

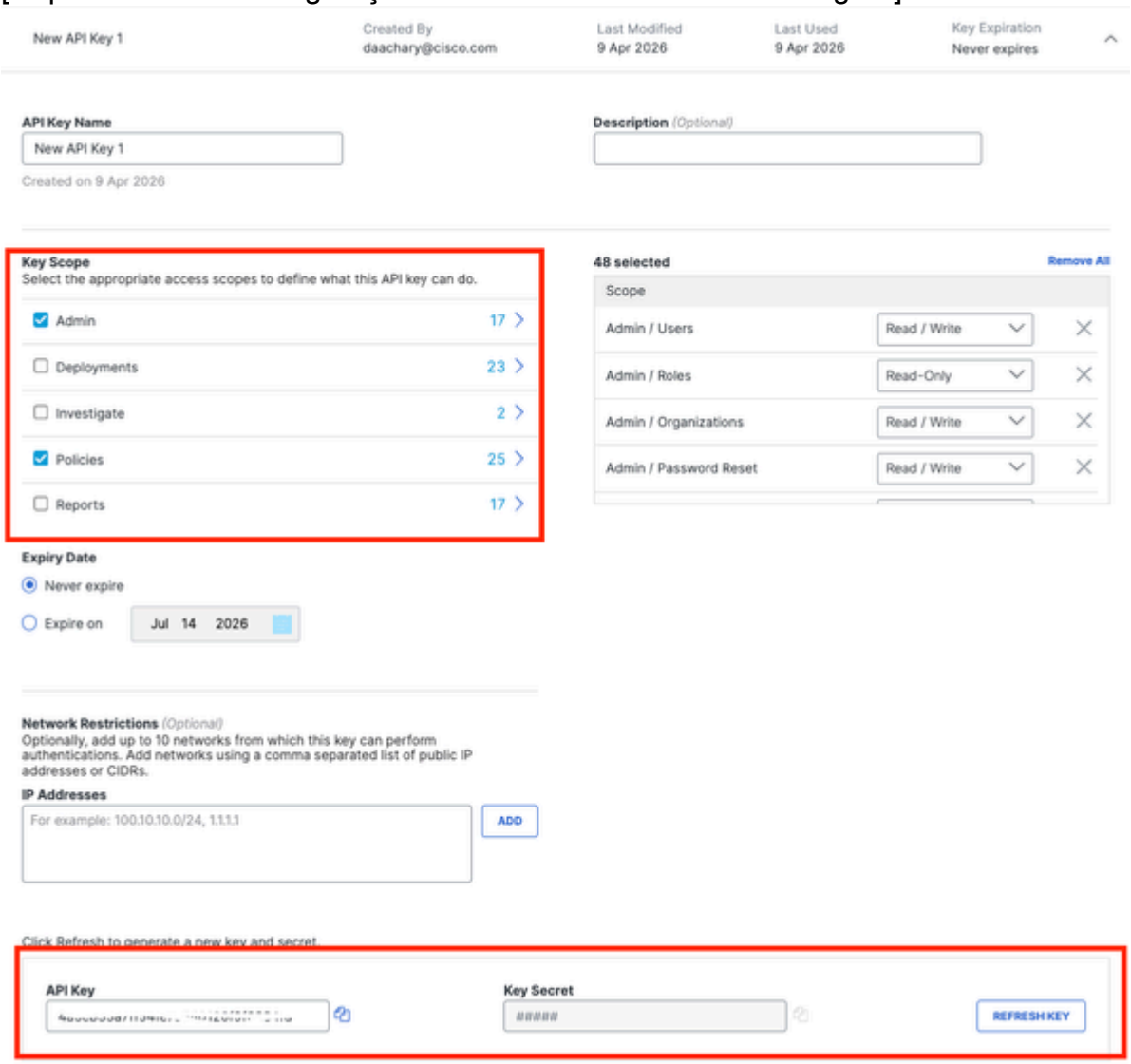
Configurar

Etapas de integração

Passo 1: Gere credenciais de API no Cisco Secure Access

Para começar, você deve gerar as credenciais de API necessárias no console do Secure Access para autorizar a conexão.

1. Faça login no painel de acesso seguro da Cisco.
2. Navegue atéAdmin>Chaves de API.
3. Selecione a opção para criar uma nova chave de API.
4. Atribua os seguintes escopos à chave:AdminandPolicy.
    - [Captura de tela: Configuração da chave de API de acesso seguro]
    -



Passo 2: Configurar Expiração de Chave

Defina o ciclo de vida da chave de API com base na política de segurança da sua organização.

- Opção 1: Nunca expirar - Fornece serviço ininterrupto sem rotação manual.
- Opção 2: Data Específica - Define um cronograma de expiração definido.
    - Nota Importante:Se você optar por definir uma data de expiração, assegure-se de planejar um processo de rotação. Você deve reconfigurar as chaves de API no console ETD antes da data de expiração para evitar uma interrupção nos serviços DLP.

Passo 3: Proteja suas credenciais

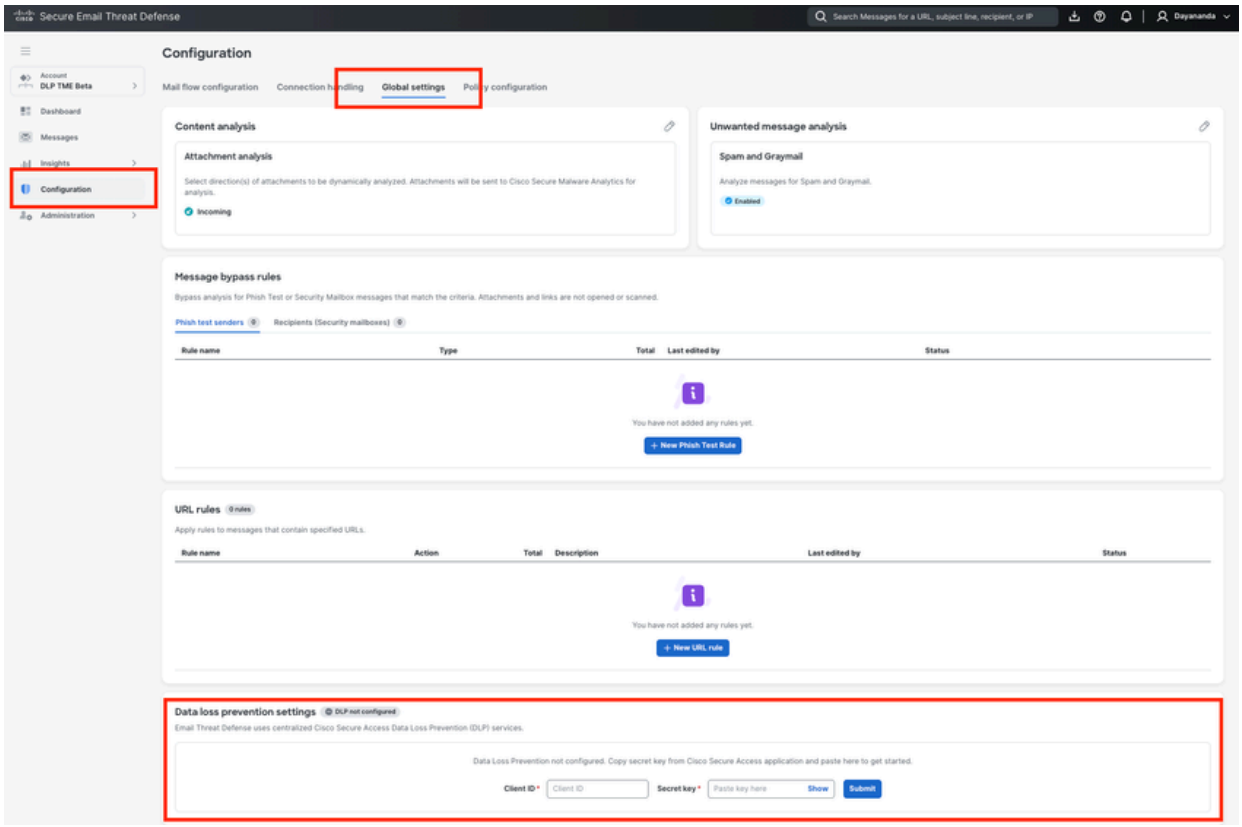
Depois que a chave for gerada, o sistema exibirá a chave da API e o segredo da chave.

- Ação:Copie e armazene essas credenciais em um local seguro (por exemplo, um gerenciador de senhas).
- Aviso:AChaveSecretnão estará visível depois que você sair desta tela. Se perder, você precisará gerar um novo par de chaves.

Passo 4: Acessar a configuração do ETD

Com suas credenciais protegidas, prossiga para o console ETD para finalizar a vinculação.

1. Faça login no console Cisco ETD.
2. Navegue até Configuration>Global Settings.
    - [Captura de tela: Configurações globais ETD [Navegação]

- 

Passo 5: Finalizar integração

Conclua o handshake inserindo as credenciais obtidas com o acesso seguro.

1. No menu Configurações globais, localize a seção Prevenção de perda de dados (DLP).
2. Insira a ID do cliente(chave de API) e aChave secreta(segredo de chave) que você salvou na Etapa 3.
3. Salve suas alterações.

Após a validação bem-sucedida, a integração entre o Cisco ETD e o Cisco Secure Access estará concluída, e suas políticas DLP estarão prontas para aplicação em todo o seu tráfego de e-mail.

Agora, a integração do ETD e do Secure Access está concluída.
NOTE: Consulte "Como configurar uma política de DLP de e-mail no Cisco Secure Access (SA) e no Cisco Email Threat Defense (ETD)"para criar uma política de DLP no Cisco Secure Access for Email DLP.

Notas Sobre Troubleshooting

Se você encontrar problemas durante ou após o processo de integração, revise os seguintes cenários comuns e etapas de correção:

1. Credenciais de API Não Aceitas no ETD

- Sintoma:Ao inserir o ID do cliente e a chave secreta no ETD, o sistema retorna um erro de autenticação.
- Resolução:
  - Verifique se a chave de API foi criada com os escopos necessários exatos:"Admin"e"Policy". Se outros escopos foram selecionados ou eles foram perdidos, a conexão falhará.
  - Certifique-se de que não haja espaços à esquerda ou à direita copiados acidentalmente ao colar a ID do cliente ou a chave secreta no console ETD.

2. Segredo chave perdido ou esquecido

- Sintoma:Você navegou para fora da tela de criação da API de acesso seguro e não pode mais exibir o segredo da chave.
- Resolução:por motivos de segurança, o segredo principal é exibido apenas uma vez no momento da criação. Se você não a salvou com segurança, exclua a chave de API incompleta no Secure Access e gere uma nova.

3. As políticas DLP não estão sendo aplicadas no tráfego de e-mail

- Sintoma:A integração é mostrada como bem-sucedida, mas as políticas de DLP configuradas não capturam nem bloqueiam e-mails confidenciais.
- Resolução:
  - Verificar Expiração da API:Se você selecionou "Selecionar uma data específica" para a expiração da chave da API (Etapa 2), verifique se a chave não expirou. Se tiver, você deverá gerar e aplicar um novo par de chaves.
  - Verificar o modo de implantação do ETD:Certifique-se de que o ETD da Cisco esteja implantado no modo em linha. O ETD deve estar no caminho do fluxo de mala direta para bloquear ou modificar ativamente as mensagens com base nos vereditos do DLP do Secure Access.
  - Tempo de sincronização:após a integração inicial, aguarde alguns minutos para que os sistemas de back-end sincronizem políticas antes de testar as regras DLP.

4. Interrupção do serviço após um período de estabilidade

- Sintoma:a aplicação de DLP pára repentinamente de funcionar após funcionar corretamente por meses.
- Resolução:Geralmente, isso é causado por uma chave de API expirada. Navegue até Admin

-> API Keyno Cisco Secure Access para verificar o status da chave usada para ETD. Implemente um processo de rotação de chaves para atualizar as credenciais em ETDantesde a data de expiração ser atingida.

Summary

A integração do Cisco Email Threat Defense (ETD) com o Cisco Secure Access (SA) é uma etapa crítica no estabelecimento de uma estratégia unificada de Prevenção de Perda de Dados (DLP). Ao gerar uma chave de API segura com escopos "Admin" e "Política" no console Secure Access e configurar essas credenciais dentro das configurações globais do ETD, os administradores criam uma ponte de comunicação transparente entre as duas plataformas.

Quando esse handshake for concluído, o ETD poderá enviar ativamente metadados de e-mail para o mecanismo DLP do Secure Access. Isso permite que a sua organização gerencie todas as políticas de proteção de dados de um único painel centralizado (acesso seguro), enquanto mantém uma visibilidade e aplicação profundas sobre o tráfego de e-mail (ETD).

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.