

Integre o acesso seguro com DLP no local usando ICAP seguro

Contents

Introdução

Este documento descreve como integrar o Acesso Seguro com servidores de Prevenção de Perda de Dados (DLP) no local usando o ICAP Seguro.

Overview

Você pode integrar o Umbrella à sua solução DLP local para fluxos de trabalho centralizados de gerenciamento de eventos e remediação. Essa integração usa o Secure ICAP (Internet Content Adaptation Protocol) para encaminhar o tráfego HTTP/S que viola as políticas DLP para o servidor DLP local para análise posterior.

Integre o acesso seguro com servidores DLP locais

- A integração usa o Secure ICAP, que transfere com segurança o tráfego HTTP/S que viola as políticas DLP para o servidor DLP local para inspeção adicional.
- O Secure ICAP criptografa o tráfego usando TLS e autentica seu servidor DLP com um certificado carregado no painel Umbrella.
- Restrinja as regras de firewall de entrada para permitir apenas o tráfego de endereços IP Umbrella para a porta ICAP do seu servidor DLP para aumentar a segurança.

Endereços IP necessários para permitir

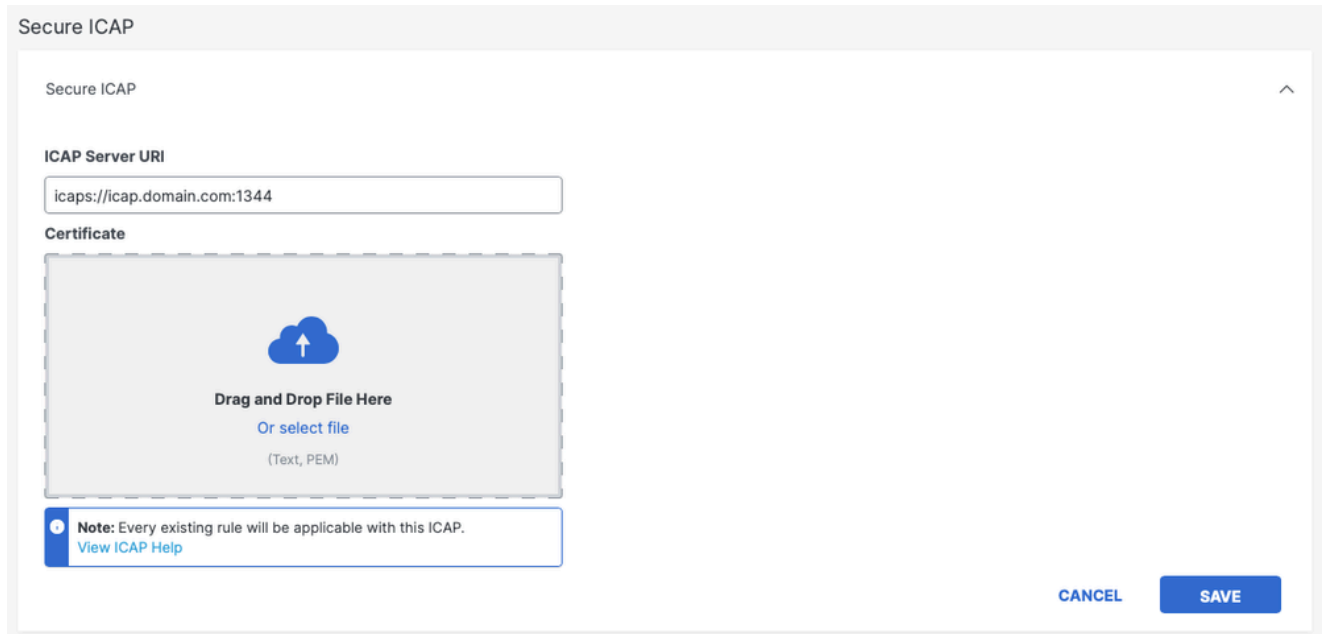
Adicione estes endereços IP Umbrella ao firewall para permitir tráfego ICAP seguro:

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Habilitar Integração ICAP Segura

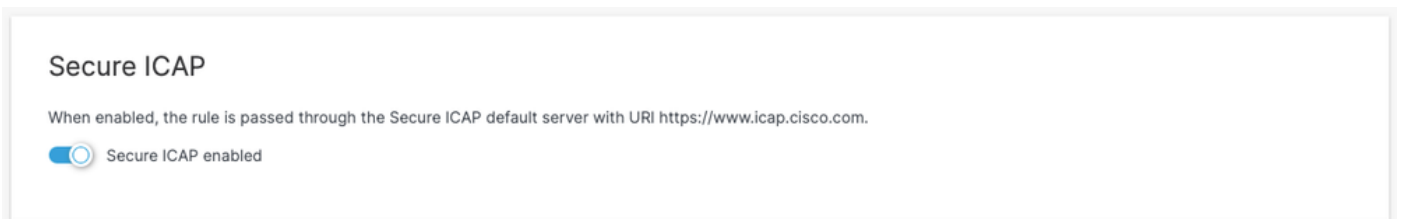
1. Integrar seu servidor DLP local:

- No painel do Umbrella, vá para Admin > Autenticação > ICAP.
- Carregue o certificado do servidor DLP para habilitar o Secure ICAP.

A screenshot of a 'Secure ICAP' configuration window. At the top, it says 'Secure ICAP' with a small upward arrow icon. Below this is the 'ICAP Server URI' field, which contains the text 'icaps://icap.domain.com:1344'. Underneath is the 'Certificate' section, which features a large dashed rectangular box. Inside this box is a blue cloud icon with an upward arrow, the text 'Drag and Drop File Here', a blue link 'Or select file', and '(Text, PEM)' in smaller text. Below the dashed box is a blue-bordered note box containing a blue circle icon, the text 'Note: Every existing rule will be applicable with this ICAP.', and a blue link 'View ICAP Help'. At the bottom right of the window are two buttons: 'CANCEL' and 'SAVE'.

2. Configure as regras de DLP em tempo real para encaminhar o tráfego para o servidor DLP local:

- Na configuração de regra, use a seção ICAP para habilitar o encaminhamento.
- Todas as regras ativas de DLP em tempo real são ativadas por padrão.

A screenshot of a 'Secure ICAP' status panel. It has the title 'Secure ICAP' and a descriptive text: 'When enabled, the rule is passed through the Secure ICAP default server with URI https://www.icap.cisco.com.' Below this text is a toggle switch that is currently turned on, followed by the text 'Secure ICAP enabled'.

Dados enviados ao servidor DLP local

- O Umbrella envia toda a mensagem HTTP/S (corpo e cabeçalhos) para o servidor DLP local.
- Os cabeçalhos personalizados estão incluídos:
 - X-Authenticated-User:Identidade do usuário
 - X-Authenticated-Groups:Identidade do grupo de usuários
 - X-Client-IP:endereço IP do cliente

Eventos de violação suportados

Os eventos de violação de DLP em tempo real monitorados e bloqueados são enviados pelo ICAP seguro.

Habilitar ICAP no Servidor DLP

Consulte a documentação e o suporte da solução DLP para habilitar o servidor ICAP incorporado.

Se somente o ICAP (não o Secure ICAP) for suportado, implante um componente de terminação TLS (como o Stunnel) na frente do servidor DLP Local para habilitar o Secure ICAP.

Recursos relacionados

Consulte a documentação do Umbrella para obter orientação adicional: [Gerenciar Secure ICAP](#)

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.