Beveiligde toegang integreren met DLP op locatie met behulp van Secure ICAP

Inhoud

Inleiding

In dit document wordt beschreven hoe u Secure Access kunt integreren met DLP-servers (Data Loss Prevention) op locatie met behulp van Secure ICAP.

Overzicht

U kunt Umbrella integreren met uw on-premises DLP-oplossing voor gecentraliseerd eventbeheer en workflows voor probleemoplossing. Deze integratie maakt gebruik van Secure ICAP (Internet Content Adaptation Protocol) om HTTP/S-verkeer dat in strijd is met het DLP-beleid door te sturen naar uw on-premises DLP-server voor verdere analyse.

Beveiligde toegang integreren met on-premises DLP-servers

- Integratie maakt gebruik van Secure ICAP, dat veilig HTTP/S-verkeer dat het DLP-beleid schendt, overbrengt naar uw on-premises DLP-server voor extra inspectie.
- Secure ICAP versleutelt verkeer met behulp van TLS en verifieert uw DLP-server met een certificaat dat is geüpload in het Umbrella-dashboard.
- Beperk de regels voor inkomende firewalls zodat alleen verkeer van Umbrella IP-adressen naar de ICAP-poort van uw DLP-server mogelijk is voor verbeterde beveiliging.

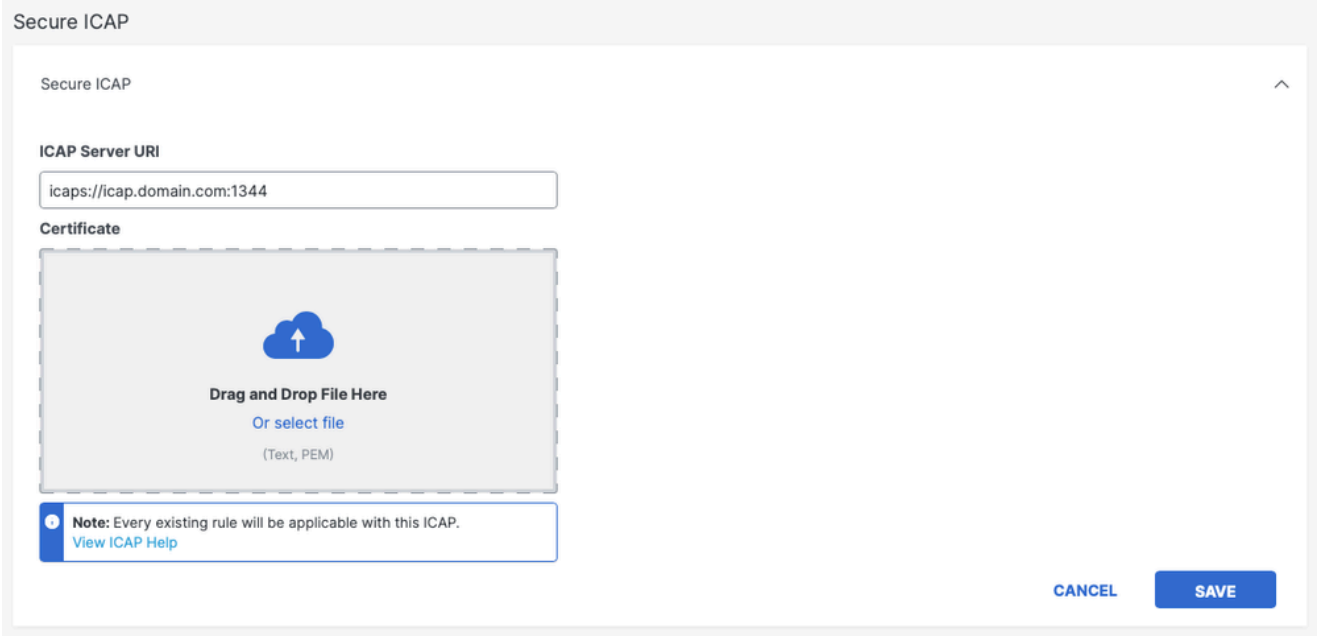
Vereiste IP-adressen om toe te staan

Voeg deze Umbrella IP-adressen toe aan uw firewall om veilig ICAP-verkeer mogelijk te maken:

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

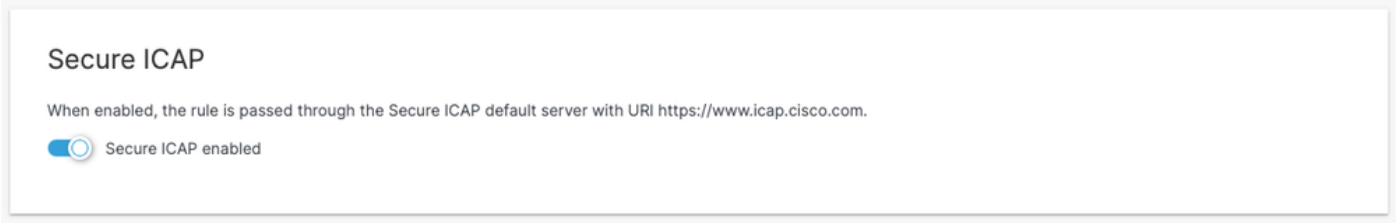
Beveiligde ICAP-integratie inschakelen

1. Aan boord van uw on-premises DLP-server:
    - Ga in het Umbrella-dashboard naar Beheer > Verificatie > ICAP.
    - Upload het DLP-servercertificaat om Secure ICAP in te schakelen.



2. Configureer realtime DLP-regels om verkeer door te sturen naar de on-premises DLP-server:

    - In de regelconfiguratie gebruikt u de sectie ICAP om doorsturen in te schakelen.
    - Alle actieve Realtime DLP-regels zijn standaard ingeschakeld.



Gegevens verzonden naar on-premises DLP-server

- Umbrella stuurt het volledige HTTP/S-bericht (body en headers) naar de on-premises DLP-server.
- Aangepaste kopteksten zijn inbegrepen:
    - X-Geverifieerde gebruiker: gebruikersidentiteit
    - X-Authenticated-Groups:identiteit gebruikersgroep
    - X-Client-IP: IP-adres van client

Ondersteunde gebeurtenissen voor overtredingen

Zowel gecontroleerde als geblokkeerde realtime DLP-inbreukgebeurtenissen worden verzonden via Secure ICAP.

ICAP inschakelen op uw DLP-server

Raadpleeg de documentatie en ondersteuning van uw DLP-oplossing om de geïntegreerde ICAP-

server in te schakelen. Als alleen ICAP (niet Secure ICAP) wordt ondersteund, implementeert u een TLS-beëindigingscomponent (zoals Stunnel) voor uw On-Premises DLP-server om Secure ICAP in te schakelen.

Gerelateerde bronnen

Raadpleeg de overkoepelende documentatie voor aanvullende richtlijnen: Secure ICAP beheren

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.