Wat is de Cisco Aggregator Server in Secure E-mail?

Inhoud

Inleiding

Dit document beschrijft wat de Cisco Aggregator Server is en hoe het werkt wanneer de Secure Email Gateway elke 30 minuten de Cisco Aggregator Server (aggregator.cisco.com poort 443) poleert voor Web Interactie Tracking-gegevens.

Wat is de Cisco Aggregator Server en hoe werkt het?

Met de Secure Email Gateway wordt de Cisco Aggregator Server (aggregator.cisco.com-poort 443) elke 30 minuten gespoeld voor Web Interactie Tracking-gegevens. Indien ingeschakeld in de functies Uitbreken en Filtering, toont het rapport Interactie Tracking van het Web deze gegevens:

- Boven geschreven kwaadaardige URL's waarop werd geklikt. Lijst van wie op de kwaadaardige URL's klikte.Tijdstempel van de klik.Als de URL is herschreven door een filter voor beleid of uitbarsting.Er wordt actie ondernomen wanneer op de URL werd gedrukt: allow, block, or onbekende.
- Topmensen die op de herschreven kwaadwillige URL's klikken.
- Web interface Tracking-details. Een lijst van alle wolken die opnieuw worden gericht en herschreven URL's.Er wordt actie ondernomen wanneer op de URL werd gedrukt: allow, block, or onbekende.

Opmerking: Zorg ervoor dat de informatie over de interactie tussen web en de gebruiker wordt weergegeven, zodat u **tegenoverliggende e-mailbeleid > Outdoorfilters** selecteert om een filter voor uitbarsting te configureren en berichtwijziging en URL-herschrijven mogelijk te maken. Configureer een contentfilter met de actie **Redirect naar Cisco Security Proxy**.

Cisco-aggregatieserver configureren

```
> aggregatorconfig

Choose the operation you want to perform:

- EDIT - Edit aggregator configuration

- CLUSTERSET - Set how aggregator is configured in a cluster.

- CLUSTERSHOW - Display how aggregator is configured in a cluster.

[]> edit

Edit aggregator address:

[aggregator.cisco.com]>

Successfully changed aggregator address to : aggregator.cisco.com
```

Hoe u Web Interactie Tracking kunt inschakelen

U kunt Web Interactie Tracking via twee verschillende functieknoppen inschakelen.

Outdoorfilters

Via de GUI:

1. Meld u aan bij de GUI van uw beveiligde e-mailgateway.
2. Over **de veiligheidsdiensten**.
3. Klik op **Outdoorfilters**.
4. Klik op **Mondiale instellingen bewerken**.
5. Controleer **Uitbraakfilters inschakelen**.
6. Controleer **Web Interactie Tracking inschakelen**.
7. Klik op **Inzenden**.
8. Klik op **Commit**.

Via de CLI:

```
> outbreakconfig

Outbreak Filters: Disabled

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.

- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.

[]> setup

Outbreak Filters: Disabled

Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.
```

```
Outbreak Filter alerts are sent when Outbreak rules cross the threshold (go above or back down
below), meaning that new messages of certain types could be

quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]> Y

What is the largest size message Outbreak Filters should scan?

[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [N]> Y

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> Y

Logging of URLs has been enabled.

Web Interaction Tracking is currently disabled.

Do you wish to enable Web Interaction Tracking? [N]> Y

Web Interaction Tracking is enabled.

The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email Security Manager in

the GUI to enable Outbreak Filters for the desired Incoming and Outgoing Mail Policies.
```

URL-filtering

Via de GUI:

1. Meld u aan bij de GUI van uw beveiligde e-mailgateway.
2. Over **de veiligheidsdiensten**.
3. Klik op **URL Filtering**.
4. Klik op **Mondiale instellingen bewerken.**
5. Controleer **URL Category en Reputation Filters inschakelen**.
6. Controleer **Web Interactie Tracking inschakelen**.
7. Klik op **Inzenden**.
8. Klik op **Commit**.

Via de CLI:

```
> websecurityconfig

Enable URL Filtering? [N]> Y

Do you wish to enable Web Interaction Tracking? [N]> Y

Web Interaction Tracking is enabled.

Do you want to add URLs to the allowed list using a URL list? [N]>
```

Web interactie-tracering

Belangrijke feiten:

- Rapportagemodules zijn niet ingevuld tenzij Web Interactie Tracking is ingeschakeld.
- Rapportage is niet in real-time ingevuld, het poleert de aggregator server en krijgt elke 30 minuten nieuwe gegevens.
- Het kan tot 2 uur duren om een klik gebeurtenis in het volgen te zien.
- Er zijn rapporten beschikbaar voor inkomende en uitgaande berichten.
- URL klikkende gebeurtenissen worden slechts gemeld als de URL door een filter van het beleid of van de Uitbarsting werd herschreven.

Als u Security Management-applicatie (SMA) gebruikt voor gecentraliseerde rapportage:

1. Meld u aan bij uw SMA.
2. Klik op het tabblad **E-mail**.
3. Over **Rapportage**.
4. Klik op **Web Interactie Tracking**.

Vastlegging cloudconnector

In recentere versies van AsyncOS, steunt de Secure Email Gateway nu de Logs van de Cloud Connector, een nieuw blogabonnement dat Web Interactie Tracking van de Cisco Aggregator Server bevat. Dit werd toegevoegd om probleemoplossing te helpen Web Interactie Tracking als zich problemen voordoen.

Via de GUI:

1. Meld u aan bij uw Secure Email Gateway GUI.
2. Over **systeembeheer**.
3. Klik op **Log Abscriptions**.

Via de CLI:

```
>logconfig

Currently configured logs:

    Log Name            Log Type                          Retrieval           Interval

-------------------------------------------------------------------------------
1. LDAP_Debug          LDAP Debug Logs                   Manual Download     None
2. audit_logs          Audit Logs                        Manual Download     None
3. cloud_connector     Cloud Connector Logs              Manual Download     None
```

Problemen oplossen

Uitgeven

Kan geen verbinding maken met de Cisco Aggregator Server.

Oplossing

1. Ping de hostnaam van de Cisco Aggregator Server van de Secure Email Gateway. U kunt het **aggregatorenig** bevel gebruiken om de hostname te vinden.
2. Controleer de proxy-verbinding die is ingesteld in **Security Services >Service updates**.

3. Controleer de firewall, de veiligheidsapparaten en het netwerk.

443	TCP	eruit	aggregator.cisco.com	Toegang tot de Cisco Aggregator-server.

- Telnet aan de aggregator van de Secure Email Gateway: telnet aggregator.cisco.com 443
- Start een pakketvastlegging naar de aggregatorserver vanaf de getroffen Secure Email Gateway.

4. Controleer DNS, en zorg ervoor dat de hostnaam van de server oplost op de Secure Email Gateway (voer dit uit op de getroffen Secure Email Gateway): nslookup aggregator.cisco.com).

Uitgeven

Kan geen webinteractie-informatie uit de Cisco Aggregator Server ophalen.

Oplossing

1. Controleer de proxy-verbinding die is ingesteld in **Security Services > Service updates**.
2. Controleer de firewall, de veiligheidsapparaten en het netwerk.

443	TCP	eruit	aggregator.cisco.com	Toegang tot de Cisco Aggregator-server.

- Telnet aan de aggregator van de Secure Email Gateway: telnet aggregator.cisco.com 443
- Start een pakketvastlegging naar de aggregatorserver vanaf de getroffen Secure Email Gateway.

3. Controleer DNS, en controleer de hostnaam van de server op het apparaat (voer dit uit op de getroffen Secure Email Gateway: nslookup aggregator.cisco.com).

Gerelateerde informatie

- Cisco Secure Email Gateway-eindgebruikershandleidingen
- Cisco Secure E-gateway release
- **Technische ondersteuning en documentatie – Cisco Systems**