¿Qué es Cisco Aggregator Server en correos electrónicos seguros?

Contenido

Introducción

Este documento describe qué es Cisco Aggregator Server y cómo funciona cuando Secure Email Gateway sondea el Cisco Aggregator Server (puerto 443 de agregador.cisco.com) cada 30 minutos para los datos de Web Interaction Tracking.

¿Qué es Cisco Aggregator Server y cómo funciona?

El gateway de correo electrónico seguro sondea el servidor de agregador de Cisco (puerto 443 de agregador.cisco.com) cada 30 minutos para los datos de rastreo de interacción web. Si se habilita en las funciones Outbreak and Filtering (Brotes y filtros), el informe de rastreo de interacción web muestra estos datos:

- Principales URL malintencionadas reescritas en las que se hizo clic. Lista de los que hicieron clic en las URL malintencionadas.Marca de tiempo del clic.Si la URL fue reescrita por un filtro de brote o política.Se realiza una acción cuando se hizo clic en la URL: permitir, bloquear o desconocer.
- Principales personas que hicieron clic en las URL malintencionadas reescritas.
- Detalles del seguimiento de interacción web. Una lista de todas las URL redirigidas y reescritas en la nube.Se realiza una acción cuando se hizo clic en la URL: permitir, bloquear o desconocer.

Nota: Para que aparezcan los Detalles de la interacción web, asegúrese de seleccionar **Políticas de correo entrante > Filtros de brote** para configurar un filtro de brote de virus y habilitar la modificación de mensajes y la reescritura de URL. Configure un filtro de contenido con la acción **Redirigir al proxy de seguridad de Cisco**.

Configuración del servidor Cisco Aggregator

```
> 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
```

Cómo Habilitar el Seguimiento de Interacción Web

Puede habilitar el rastreo de interacción web a través de dos configuraciones de funciones diferentes.

Filtros de brote

A través de la GUI:

1. Inicie sesión en la GUI de Secure Email Gateway.
2. Pase el cursor sobre **Servicios de seguridad**.
3. Haga clic en **Filtros de brote de virus**.
4. Haga clic en **Editar configuración global**.
5. Marque **Enable Outbreak Filters**.
6. Marque **Enable Web Interaction Tracking**.
7. Haga clic en Submit (Enviar).
8. Haga clic en **Confirmar**.

A través de la 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.
```

Filtrado de URL

A través de la GUI:

1. Inicie sesión en la GUI de Secure Email Gateway.
2. Pase el cursor sobre **Servicios de seguridad**.
3. Haga clic en **Filtrado de URL**.
4. Haga clic en **Editar configuración global.**
5. Marque **Habilitar categoría de URL y filtros de reputación**.
6. Marque **Enable Web Interaction Tracking**.
7. Haga clic en Submit (Enviar).
8. Haga clic en **Confirmar**.

A través de la 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]>
```

Seguimiento de interacción web

Datos importantes:

- Los módulos de informes no se rellenan a menos que esté habilitado el rastreo de interacción web.
- Los informes no se rellenan en tiempo real, sondea el servidor del agregador y obtiene nuevos datos cada 30 minutos.
- Puede tardar hasta 2 horas en ver un evento de clic en el seguimiento.
- Los informes están disponibles para los mensajes entrantes y salientes.
- Los eventos de clic de URL se notifican sólo si la URL fue reescrita por un filtro de política o brote de virus.

Si utiliza Security Management Appliance (SMA) para la generación de informes centralizada:

1. Inicie sesión en el SMA.
2. Haga clic en la pestaña **Correo electrónico**.
3. Pase el cursor sobre **Reporting**.
4. Haga clic en **Web Interaction Tracking**.

Registro del conector de nube

En las versiones más recientes de AsyncOS, Secure Email Gateway admite ahora los registros de conectores de nube, una nueva suscripción de registro que contiene el seguimiento de interacción web del servidor Cisco Aggregator. Esto se agregó para ayudar a resolver problemas de rastreo de interacción web si se producen problemas.

A través de la GUI:

1. Inicie sesión en la GUI de Secure Email Gateway.
2. Pase el cursor sobre **Administración del sistema**.
3. Haga clic en **Suscripciones de registro**.

A través de la 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
```

Troubleshoot

Problema

No se puede conectar al servidor de agregador de Cisco.

Solución

1. Haga ping en el nombre de host del servidor de agregador de Cisco desde el gateway de correo electrónico seguro. Puede utilizar el comando **aggregatorconfig** para encontrar el nombre de host.
2. Verifique la conexión proxy configurada en **Servicios de Seguridad > Actualizaciones de Servicio**.
3. Compruebe el firewall, los dispositivos de seguridad y la red.

443 TCP FUERA aggregator.cisco.com Acceso al servidor Cisco Aggregator.

- Telnet al servidor de agregador desde el gateway de correo electrónico seguro: telnet aggregator.cisco.com 443
- Ejecute una captura de paquetes en el servidor de agregador desde el gateway de correo electrónico seguro afectado.

4. Verifique DNS, asegúrese de que el nombre de host del servidor resuelva en el gateway de correo electrónico seguro (ejecute esto en el gateway de correo electrónico seguro afectado: nslookup aggregator.cisco.com).

Problema

No se puede recuperar la información de seguimiento de la interacción web del servidor de agregador de Cisco.

Solución

1. Verifique la conexión proxy configurada en **Servicios de Seguridad > Actualizaciones de Servicio**.
2. Compruebe el firewall, los dispositivos de seguridad y la red.

443 TCP FUERA aggregator.cisco.com Acceso al servidor Cisco Aggregator.

- Telnet al servidor de agregador desde el gateway de correo electrónico seguro: telnet aggregator.cisco.com 443
- Ejecute una captura de paquetes en el servidor de agregador desde el gateway de correo electrónico seguro afectado.

3. Verifique DNS, asegúrese de que el nombre de host del servidor resuelva en el dispositivo (ejecute esto en el gateway de correo electrónico seguro afectado: nslookup aggregator.cisco.com).

Información Relacionada

- Guías de usuario final de Cisco Secure Email Gateway
- Notas de la versión de Cisco Secure Email Gateway
- **Soporte Técnico y Documentación - Cisco Systems**