Cos'è Cisco Aggregator Server in Secure Email?

Sommario

Introduzione

Questo documento descrive cos'è Cisco Aggregator Server e come funziona quando Secure Email Gateway esegue il polling a Cisco Aggregator Server (aggregator.cisco.com porta 443) ogni 30 minuti per i dati di Web Interaction Tracking.

Che cos'è Cisco Aggregator Server e come funziona?

Secure Email Gateway esegue il polling del Cisco Aggregator Server (aggregator.cisco.com porta 443) ogni 30 minuti per i dati di Web Interaction Tracking. Se abilitato nelle funzionalità Epidemie e Filtro, il report Tracciamento interazione Web mostra i seguenti dati:

- Principali URL dannosi riscritti su cui è stato fatto clic. Elenco degli utenti che hanno fatto clic sugli URL dannosi.Timestamp del clic.Se l'URL è stato riscritto da un filtro criteri o epidemie.L'azione viene eseguita quando si fa clic sull'URL: consenti, blocca o sconosciuto.
- Principali persone che hanno fatto clic sugli URL dannosi riscritti.
- Dettagli tracciabilità interazione Web. Elenco di tutti gli URL reindirizzati e riscritti del cloud.L'azione viene eseguita quando si fa clic sull'URL: consenti, blocca o sconosciuto.

Nota: Per visualizzare i dettagli dell'interazione Web, selezionare **Policy di posta in arrivo > Filtri epidemie** per configurare un filtro epidemie e abilitare la modifica dei messaggi e la riscrittura dell'URL. Configurare un filtro contenuti con l'azione **Reindirizza a Cisco Security Proxy**.

Configurazione di Cisco Aggregator Server

```
> 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
```

Come abilitare il rilevamento delle interazioni Web

Èpossibile attivare il rilevamento delle interazioni Web mediante due diverse configurazioni di funzionalità.

Filtri epidemie

Dalla GUI:

1. Accedere alla GUI di Secure Email Gateway.
2. Passare il mouse sui **servizi di sicurezza**.
3. Fare clic su **Filtri epidemie**.
4. Fare clic su **Modifica impostazioni globali**.
5. Selezionare **Enable Outbreak Filters**.
6. Selezionare **Abilita rilevamento interazione Web**.
7. Fare clic su **Invia**.
8. Fare clic su **Conferma**.

Dalla 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.
```

Filtro URL

Dalla GUI:

1. Accedere alla GUI di Secure Email Gateway.
2. Passare il mouse sui **servizi di sicurezza**.
3. Fare clic su **URL Filtering (Filtro URL)**.
4. Fare clic su **Modifica impostazioni globali.**
5. Selezionare **Enable URL Category and Reputation Filters (Abilita filtri categorie URL e reputazione)**.
6. Selezionare **Abilita rilevamento interazione Web**.
7. Fare clic su **Invia**.
8. Fare clic su **Conferma**.

Dalla 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]>
```

Tracciamento interazione Web

Fatti importanti:

- I moduli di report non vengono popolati a meno che il rilevamento interazione Web non sia

abilitato.
- Il report non viene compilato in tempo reale, esegue il polling del server di aggregazione e ottiene nuovi dati ogni 30 minuti.
- La visualizzazione di un evento Click nel rilevamento può richiedere fino a 2 ore.
- Sono disponibili rapporti per i messaggi in arrivo e in uscita.
- Gli eventi di selezione URL vengono segnalati solo se l'URL è stato riscritto da un filtro criteri o epidemie.

Se si utilizza Security Management Appliance (SMA) per il reporting centralizzato:

1. Accedere all'SMA.
2. Fare clic sulla scheda **Email**.
3. Passare il mouse su **Reporting**.
4. Fare clic su **Tracciamento interazione Web**.

Registrazione connettore cloud

Nelle versioni più recenti di AsyncOS, Secure Email Gateway supporta ora Cloud Connector Logs, una nuova sottoscrizione di log che contiene Web Interaction Tracking di Cisco Aggregator Server. Questa opzione è stata aggiunta per facilitare la risoluzione dei problemi relativi al rilevamento delle interazioni Web in caso di problemi.

Dalla GUI:

1. Accedere alla GUI di Secure Email Gateway.
2. Passare il mouse su **Amministrazione sistema**.
3. Fare clic su **Registra sottoscrizioni**.

Dalla 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
```

Risoluzione dei problemi

Problema

Impossibile connettersi al server Cisco Aggregator.

Soluzione

1. Eseguire il ping del nome host del server Aggregator Cisco dal gateway di posta elettronica sicura. È possibile usare il comando **aggregatorconfig** per trovare il nome host.
2. Verificare la connessione proxy configurata in **Servizi di sicurezza > Aggiornamenti servizi**.

3. Controllare il firewall, i dispositivi di sicurezza e la rete.

443	TCP	Uscita	aggregator.cisco.com	Accedere al server Cisco Aggregator.

- Telnet su server di aggregazione dal gateway Secure Email: telnet aggregator.cisco.com 443
- Eseguire un'acquisizione pacchetti sul server aggregator dal gateway di posta elettronica sicura interessato.

4. Controllare il DNS, accertarsi che il nome host del server sia risolto nel gateway di posta elettronica sicura (eseguire questa operazione sul gateway di posta elettronica sicura interessato: nslookup aggregator.cisco.com).

Problema

Impossibile recuperare le informazioni di rilevamento dell'interazione Web da Cisco Aggregator Server.

Soluzione

1. Verificare la connessione proxy configurata in **Servizi di sicurezza > Aggiornamenti servizi**.
2. Controllare il firewall, i dispositivi di sicurezza e la rete.

443	TCP	Uscita	aggregator.cisco.com	Accedere al server Cisco Aggregator.

- Telnet su server di aggregazione dal gateway Secure Email: telnet aggregator.cisco.com 443
- Eseguire un'acquisizione pacchetti sul server aggregator dal gateway di posta elettronica sicura interessato.

3. Controllare il DNS, accertarsi che il nome host del server sia risolto nell'accessorio (eseguire questa operazione sul gateway di posta elettronica sicuro interessato: nslookup aggregator.cisco.com).

Informazioni correlate

- Guide per l'utente finale di Cisco Secure Email Gateway
- Note sulla release di Cisco Secure Email Gateway
- **Documentazione e supporto tecnico – Cisco Systems**