Secure Email에서 Cisco Aggregator Server란 무엇입니까?

목차

소개

이 문서에서는 Cisco Aggregator Server의 특징 및 Secure Email Gateway가 Cisco Aggregator Server(aggregator.cisco.com 포트 443)를 30분마다 Web Interaction Tracking 데이터에 폴링할 때의 작동 방식에 대해 설명합니다.

Cisco Aggregator Server란 무엇이며 어떻게 작동합니까?

Secure Email Gateway는 Web Interaction Tracking 데이터를 위해 30분마다 Cisco Aggregator Server(aggregator.cisco.com 포트 443)를 폴링합니다.Outbreak and Filtering(아웃브레이크 및 필터링) 기능에서 활성화된 경우 Web Interaction Tracking(웹 상호 작용 추적) 보고서에는 다음 데이터가 표시됩니다.

- 클릭된 상위 재작성된 악성 URL입니다. 악성 URL을 클릭한 사용자 목록클릭의 타임스탬프입니다.URL이 정책 또는 Outbreak 필터에 의해 재작성된 경우.URL을 클릭하면 허용, 차단 또는 알 수 없는 작업이 수행됩니다.
- 재작성된 악성 URL을 클릭한 상위 사용자
- 웹 상호 작용 추적 세부 정보 리디렉션되고 재작성된 모든 클라우드 URL 목록URL을 클릭하면 허용, 차단 또는 알 수 없는 작업이 수행됩니다.

참고: Web Interaction Details(웹 상호작용 세부사항)가 표시되려면 Outbreak(보안 침해) 필터를 구성하고 메시지 수정 및 URL 재작성을 활성화하려면 Incoming **Mail Policies(수신 메일 정책)** > **Outbreak Filters(신종 바이러스 필터)**를 선택해야 합니다.**Redirect to Cisco Security Proxy** 작업을 사용하여 콘텐츠 필터**를** 구성합니다.

Cisco Aggregator 서버 구성

```
> 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
```

웹 상호 작용 추적을 활성화하는 방법

두 가지 다른 기능 컨피그레이션을 통해 웹 상호 작용 추적을 활성화할 수 있습니다.

신종 바이러스 필터

GUI를 통해 다음을 수행합니다.

1. Secure Email Gateway의 GUI에 로그인합니다.
2. **보안 서비스**에 마우스를 **놓습니다**.
3. Outbreak **Filters를 클릭합니다**.
4. Edit **Global Settings를 클릭합니다**.
5. Enable **Outbreak Filters를 선택합니다**.
6. Enable **Web Interaction Tracking(웹 상호 작용 추적 활성화)을 선택합니다**.
7. Submit(제출)**을 클릭합니다**.
8. Commit을 **클릭합니다**.

CLI를 통해 다음을 수행합니다.

```
> 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 필터링

GUI를 통해 다음을 수행합니다.

1. Secure Email Gateway의 GUI에 로그인합니다.
2. **보안 서비스**에 마우스를 **놓습니다**.
3. **URL Filtering(URL 필터링)을 클릭합니다**.
4. Edit **Global Settings를 클릭합니다.**
5. Enable **URL Category and Reputation Filters(URL 범주 및 평판 필터 활성화)를 선택합니다**.
6. Enable **Web Interaction Tracking(웹 상호 작용 추적 활성화)을 선택합니다**.
7. Submit(제출)**을 클릭합니다**.
8. Commit을 **클릭합니다**.

CLI를 통해 다음을 수행합니다.

```
> 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]>
```

웹 상호 작용 추적

중요한 사실:

- Web Interaction Tracking(웹 상호 작용 추적)이 활성화되어 있지 않으면 보고 모듈이 채워지지

않습니다.
- 보고는 실시간으로 채워지지 않으며 집계 서버를 폴링하고 30분마다 새 데이터를 얻습니다.
- 추적에서 클릭 이벤트를 보려면 최대 2시간이 걸릴 수 있습니다.
- 수신 및 발신 메시지에 대해 보고서를 사용할 수 있습니다.
- URL 클릭 이벤트는 URL이 정책 또는 Outbreak 필터에 의해 재작성된 경우에만 보고됩니다.

중앙 집중식 보고에 SMA(Security Management Appliance)를 사용하는 경우

1. SMA에 로그인합니다.
2. **이메일** 탭을 클릭합니다.
3. **보고** 위에 마우스 **커서를 놓습니다**.
4. Web **Interaction Tracking을 클릭합니다**.

클라우드 커넥터 로깅

최신 버전의 AsyncOS에서 Secure Email Gateway는 이제 Cisco Aggregator Server의 Web Interaction Tracking을 포함하는 새로운 로그 서브스크립션인 클라우드 커넥터 로그를 지원합니다 .문제가 발생할 경우 웹 상호 작용 추적 문제를 해결하는 데 도움이 되도록 추가되었습니다.

GUI를 통해 다음을 수행합니다.

1. 보안 이메일 게이트웨이 GUI에 로그인합니다.
2. **시스템 관리** 위에 **마우스 커서를 놓습니다**.
3. Log Subscriptions(**로그 서브스크립션)를 클릭합니다**.

CLI를 통해 다음을 수행합니다.

```
>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
```

문제 해결

문제

Cisco Aggregator Server에 연결할 수 없습니다.

솔루션

1. Secure Email Gateway에서 Cisco Aggregator Server의 호스트 이름을 ping합니다.호스트 이름을 찾기 위해 **aggregatorconfig** 명령을 사용할 수 있습니다.
2. Security Services(**보안 서비스)>** Service Updates(서비스 업데이트)에서 구성된 프록시 연결**을 확인합니다**.
3. 방화벽, 보안 디바이스 및 네트워크를 확인합니다.

443 TCP 출력 aggregator.cisco.com Cisco Aggregator 서버에 액세스합니다.

- Secure Email Gateway에서 Aggregator 서버에 텔넷:telnet aggregator.cisco.com 443
- 영향을 받는 Secure Email Gateway에서 Aggregator 서버로 패킷 캡처를 실행합니다.

4. DNS를 선택하고 서버의 호스트 이름이 보안 이메일 게이트웨이에서 확인되는지 확인합니다(영향을 받는 보안 이메일 게이트웨이에서 실행:nslookup aggregator.cisco.com).

문제

Cisco Aggregator Server에서 웹 상호 작용 추적 정보를 검색할 수 없습니다.

솔루션

1. **Security Services(보안 서비스)** > Service Updates(**서비스 업데이트)**에서 구성된 프록시 연결을 **확인합니다**.
2. 방화벽, 보안 디바이스 및 네트워크를 확인합니다.

443 TCP 출력 aggregator.cisco.com Cisco Aggregator 서버에 액세스합니다.

- Secure Email Gateway에서 Aggregator 서버에 텔넷:telnet aggregator.cisco.com 443
- 영향을 받는 Secure Email Gateway에서 Aggregator 서버로 패킷 캡처를 실행합니다.

3. DNS를 선택하고 서버의 호스트 이름이 어플라이언스에서 확인되는지 확인합니다(영향을 받는 보안 이메일 게이트웨이에서 실행:nslookup aggregator.cisco.com).

관련 정보

- Cisco Secure Email Gateway 최종 사용자 가이드
- Cisco Secure Email Gateway 릴리스 정보
- **기술 지원 및 문서 – Cisco Systems**