

SEG에 대한 위협 스캐너 정책 단위 검사 구성

목차

[소개](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[구성](#)

[웹 인터페이스 설정](#)

[명령줄 인터페이스 설정](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Cisco SEG(Secure Email Gateway)에 대한 TS(Threat Scanner) Per Policy Integration의 서비스 및 컨피그레이션에 대해 설명합니다.

사전 요구 사항

SEG 일반 설정 및 구성에 대한 지식이 필요합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco SEG(Secure Email Gateway) AsyncOS 15.5.1 이상
- 그레이메일 서비스.
- 안티스팸 서비스.
- 수신 메일 정책.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

그레이메일 서비스의 새롭게 활성화된 하위 구성 요소인 TS(Threat Scanner)는 AntiSpam 탐지의 효과를 더욱 높여주는 AntiSpam CASE와 통합되었습니다.

그레이메일 서비스가 활성화되면 Threat Scanner를 활성화하는 옵션이 각 Incoming Mail Policy AntiSpam 설정에서 활성화됩니다. TS는 HTML 밀수 탐지에 중점을 두고 전반적인 안티스팸 탐지 기능을 개선했습니다.

- HTML 구문 분석 및 악성 스크립트 탐지
- URL 구문 분석 및 리디렉션 탐지

Antispam CASE 엔진은 업데이트 및 스팸 확정을 관리하면서 두 서비스를 제어합니다.

TS는 각 수신 메일 정책 안티스팸 설정 내에서 활성화/비활성화 설정을 표시합니다.

TS는 판결에 영향을 미쳐 최종 Antispam CASE 판정의 비중을 높입니다.

구성


컨피그레이션은 Enable Graymail Detection(그레이메일 탐지 활성화) 및 Enabling TS within the Incoming Mail Policies(수신 메일 정책 내에서 TS 활성화)의 두 가지 작업으로 구성됩니다.

- TS를 활성화하려면 그레이메일 글로벌 서비스를 활성화해야 합니다.
- 그레이메일이 전역적으로 활성화되면 인바운드 메일 정책 "Antispam" 옵션인 "Enable Threat Scanner"를 사용할 수 있습니다.


웹 인터페이스 설정

WebUI 내에서 그레이메일을 활성화하려면

- Security services(보안 서비스)로 이동
 - IMS 및 그레이메일
 - 그레이메일 전역 설정
 - 그레이메일 설정을 수정합니다.
 - 그레이메일 탐지를 활성화하는 옵션을 선택합니다.
- 변경 사항을 제출 및 커밋하여 작업을 마무리합니다.

Graymail Global Settings	
Graymail Detection	Disabled 
Safe Unsubscribe	Disabled

[Edit Graymail Settings](#)

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input checked="" type="checkbox"/> Enable Threat Scanner  <i>You must enable Graymail Global Settings to enable Threat Scanner.</i> <input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

[설정 전 보기](#)

그레이메일이 활성화되면 Threat Scanner(위협 스캐너) 선택 상자를 각 수신 메일 정책에 사용할 수 있게 됩니다.

WebUI 내에서 Threat Scanner를 활성화하려면

- Mail Policies(메일 정책)로 이동
 - 수신 메일 정책
 - 원하는 메일 정책 선택
 - Anti-Spam을 선택합니다.
 - 컨피그레이션 페이지의 상단에는 Enable Threat Scanner(Threat Scanner 활성화)에 대한 확인란 옵션이 표시됩니다.
- 변경 사항을 제출 및 커밋하여 컨피그레이션 완료

Graymail Global Settings	
Graymail Detection	Enabled ←
Safe Unsubscribe	Disabled
Automatic Updates (?)	Enabled

[Edit Graymail Settings](#)

Anti-Spam Settings	
	Policy: Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service
	<input checked="" type="checkbox"/> Enable Threat Scanner ←
	<input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i>
	<input type="radio"/> Disabled

안티스팸 내의 위협 스캐너 옵션

명령줄 인터페이스 설정

CLI 명령을 사용하여 그레이메일 서비스를 활성화합니다.

- `imsandgraymailconfig`
 - 그레이메일
 - 설정
 - 그레이메일 탐지를 사용하시겠습니까? [Y] >
 - 그레이메일 엔진에 대한 자동 업데이트를 활성화하시겠습니까? [Y]>
 - 나머지 프롬프트를 완료하여 기본 머신 프롬프트로 돌아갑니다.
- Commit + 원하는 코멘트를 추가 > "Return" 키를 눌러 작업을 완료합니다.

CLI에서 정책 내 위협 스캐너 활성화 또는 비활성화

- CLI > policy 컨피그레이션

Incoming Mail Policy(수신 메일 정책) 또는 Outgoing Mail Policies(발신 메일 정책) 또는 Match Headers Priority(헤더 우선순위 일치)를 구성하시겠습니까?

1. 수신 메일 정책
2. 발송 메일 정책
3. 헤더 우선 순위 일치

[1]> 1

수신 메일 정책 컨피그레이션

1. 북쪽1
2. BLOCKED_LIST
3. 허용 목록
4. ALLOW_SPOOF
5. 기본값

편집할 항목의 이름 또는 번호를 입력합니다.

[]> 1

수행할 작업을 선택합니다.

- NAME - 정책 이름 변경
- NEW - 새 정책 구성원 행 추가
- 삭제 - 정책 구성원 행 제거
- 인쇄 - 정책 구성원 행 인쇄
- 안티스팸 - 안티스팸 정책 수정
- 안티바이러스 - 안티바이러스 정책 수정
- OUTBREAK - Outbreak Filter 정책 수정
- ADVANCEDMALWARE - Advanced Malware Protection 정책 수정
- 그레이메일 - 그레이메일 정책 수정
- THREATDEFENSECONNECTOR - Threat Defense 커넥터 수정
- 필터 - 필터 수정

[]> 안티스팸

수행할 작업을 선택합니다.

- DISABLE - Anti-Spam 정책 비활성화(모든 정책 관련 작업 비활성화)
- ENABLE - 안티스팸 정책 활성화

[]> 사용

안티스팸 구성 시작

이 정책에서 Intelligent Multi-Scan을 사용하시겠습니까? [N]>

이 정책에서 IronPort Anti-Spam을 사용하시겠습니까? [Y]>

일부 메시지는 스팸으로 식별됩니다. 일부 메시지는 의심스런 스팸으로 식별됩니다. IronPort 안티스팸 의심 스팸을 설정할 수 있습니다. 임계값 미만입니다.

구성 옵션은 다음과 같이 긍정적으로 식별된 메시지에 적용됩니다.

스팸:

Threat Scanner 판정에 대한 특별 처리를 사용하도록 설정하시겠습니까? [N]> y

메뉴 선택을 계속 진행하여 메일 정책 선택을 완료하고 "반환 키"를 눌러 각 선택 항목에 대한 기본 작업을 적용합니다.

명령을 사용하여 저장을 완료합니다.

- Commit + 원하는 코멘트를 추가 > "Return" 키를 눌러 작업을 완료합니다.

다음을 확인합니다.

로그를 읽고 해석하는 방법.

Threat Scanner의 Mail Logging은 중간 판정만 표시하고 CASE는 최종 판정을 표시합니다.

메일 로그는 정상 판결과 유죄 판정의 위협 스캐너 판정에 대한 두 가지 다른 버전을 보여줍니다

- Threat Scanner Interim 판정이 clean(정상)인 경우 이 샘플과 유사하게 로그가 표시됩니다.
 - 정보: 중간 그레이메일 판정 - LEGIT(0) <정상 메시지>
 - 정보: 중간 그레이메일 판정 - MCE (11) <기타 이메일 캠페인>
- Threat Scanner Interim 판정에서 유죄를 판정할 경우 이 샘플과 유사하게 로그가 표시됩니다.
 - 정보: 중간 ThreatScanner 판정 - 피싱(101)
 - 정보: 중간 ThreatScanner 판정 - 바이러스 (2)

메일 로그 샘플: Threat Scanner Clean(위협 스캐너 정상) 판정에서는 다른 용어(그레이메일 판정)를 사용합니다.

<#root>

Wed Jan 31 08:19:32 2024 Info: MID 3189755

interim graymail verdict - LEGIT (0) <Clean message>

Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative

Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative

Message Tracking(메시지 추적)에는 Threat Scanner 로그 항목이 표시되지 않으며 CASE: Final Verdict(CASE: 최종 판정)만 표시됩니다.

TS(Threat Scanner)의 이러한 샘플은 4가지 판정 시나리오를 제공합니다.



참고: "피싱" 및 "바이러스"의 TS 범주가 CASE 판정의 비중을 높이는 유일한 탐지입니다

메일 로그 샘플: PHISHING TS Conviction 및 AntiSpam Conviction 모두 있음

<#root>

Thu Jan 25 09:05:23 2024 Info: MID 3057397

interim

ThreatScanner verdict - PHISHING (101)

<Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>

Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive

Thu Jan 25 09:05:23 2024 Info: MID 3057397

using engine: CASE spam positive

Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE

추적 샘플: PHISHING TS Conviction이 없고 CASE Conviction이 있습니다.

25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive

피싱 TS 기결수 및 안티스팸 기결수 추적

메일 로그 샘플: PHISHING TS Conviction 및 AntiSpam Negative가 모두 존재합니다.

<#root>

Thu Jan 25 09:05:47 2024 Info: MID 3057413

interim ThreatScanner verdict - PHISHING (101)

<Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>

Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative

Thu Jan 25 09:05:47 2024 Info: MID 3057413

using engine: CASE spam negative

추적 샘플: 피싱 TS Configured 및 AntiSpam Negative가 있습니다.

25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative

메일 로그 샘플: 메일 로그의 VIRUS TS Conviction 및 AntiSpam Conviction 샘플.

<#root>

Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim

ThreatScanner verdict - VIRUS (2)

```
<Virus detected by ThreatScanner engine>
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive
Thu Jan 25 13:37:16 2024 Info: MID 3066060
using engine: CASE spam positive
```

Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE

추적 샘플: VIRUS TS Conviction 없음 및 AntiSpam Conviction 있음

```
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00) Message 3066060 aborted: Dropped by CASE
```

메일 로그 샘플: VIRUS TS Conviction 및 AntiSpam Negative가 모두 존재합니다.

<#root>

Jan 23 21:38:57 2024 Info: MID 3013692

interim ThreatScanner verdict - VIRUS (2)

```
<Virus detected by ThreatScanner engine>
Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative
Jan 23 21:38:58 2024 Info: MID 3013692
using engine: CASE spam negative
```

추적 샘플: VIRUS TS Conviction 없음 및 AntiSpam Negative 있음

```
23 Jan 2024 19:38:57 (GMT -08:00) Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00) Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00) Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative
```

그레이메일 로그에는 Threat Scanner 판정과 거짓 긍정(false positive) 문제가 발생하는 경우 TALOS 분석을 위한 지원 콘텐츠가 포함되어 있습니다.

Threat Scanner raw 결과가 있으면 그레이메일 로깅이 더 빠르게 롤오버됩니다. 이 동작을 해결하기 위해 그레이메일 로그에 대한 SEG 수정이 수행되었습니다.

- AsyncOS 15.5에서는 로그 보존 수준을 높이기 위해 그레이메일 로그 파일에 대한 Default Log Subscription을 20으로 설정합니다.
 - 업그레이드 시 설정이 20보다 높게 설정된 경우 로그 파일 설정이 변경되지 않습니다.
- 인바운드 그레이메일 Interim Configured 메시지는 정보 레벨에서 전체 스캔 원시 결과를 표시합니다.
- 다른 모든 메시지에 대한 그레이메일 검사 결과는 디버그 레벨에 표시됩니다.

관련 정보

- [이메일 보안 설정 가이드](#)
- [Cisco Secure Email Gateway 시작 페이지 - 지원 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.