Secure Email Gateway 및 클라우드 게이트웨이에 대한 URL 필터링 설정

목차

소개

이 문서에서는 Cisco Secure Email Gateway 및 Cloud Gateway에서 URL 필터링을 구성하는 방법과 URL 필터링 사용에 대한 모범 사례에 대해 설명합니다.

배경 정보

URL 필터링은 AsyncOS 11.1 for Email Security에 처음 도입되었습니다. 이 릴리스에서는 Cisco Secure Email을 구성하여 메시지 첨부 파일의 URL을 검사하고 이러한 메시지에 대해 구성된 작업을 수행할 수 있었습니다. 메시지 및 콘텐츠 필터는 URL 평판 및 URL 카테고리를 사용하여 메시지 및 첨부 파일의 URL을 확인합니다. 자세한 내용은 사용 설명서 또는 온라인 도움말의 "메시지 필터를 사용하여 이메일 정책 적용", "콘텐츠 필터" 및 "신뢰할 수 없거나 바람직하지 않은 URL로부터 보호" 장을 참조하십시오.

신뢰할 수 없거나 바람직하지 않은 링크에 대한 제어 및 보호는 안티스팸, 보안 침해, 콘텐츠 및 메시지 필터링 프로세스를 위해 작업 대기열에 통합됩니다. 이를 통해 다음을 제어합니다.

- 메시지 및 첨부 파일에서 신뢰할 수 없는 URL로부터 보호하는 효과를 높입니다.
- 또한 URL 필터링은 Outbreak Filter에 통합됩니다. 이와 같이 강화된 보호 기능은 조직에서 이미 Cisco Web Security Appliance를 보유하고 있거나 웹 기반 위협으로부터 유사한 보호 기능을 보유하고 있는 경우에도 적용할 수 있습니다. 이는 진입 지점에서 위협을 차단하기 때문입니다.
- 콘텐츠 또는 메시지 필터를 사용하여 메시지에 있는 URL의 WBRS(Web-Based Reputation Score)를 기반으로 작업을 수행할 수도 있습니다. 예를 들어, 평판이 중립이거나 알 수 없는 URL을 재작성하여 클릭 시 안전 평가를 위해 Cisco Web Security Proxy로 리디렉션할 수 있습니다.
- 스팸을 더 잘 식별
- 어플라이언스는 스팸 식별을 돕기 위해 메시지 및 기타 스팸 식별 알고리즘에 있는 링크의 평판 및 카테고리를 사용합니다. 예를 들어, 메시지의 링크가 마케팅 웹 사이트에 속하는 경우 해당 메시지는 마케팅 메시지일 가능성이 높습니다.
- 기업에서 허용되는 사용 정책의 시행 지원
- URL 범주(성인 콘텐츠 또는 불법 활동 등)를 콘텐츠 및 메시지 필터와 함께 사용하여 허용되는 기업 사용 정책을 적용할 수 있습니다.
- 조직에서 보호를 위해 다시 작성된 메시지의 URL을 가장 자주 클릭한 사용자와 가장 자주 클릭한 링크를 식별할 수 있습니다.

참고: AsyncOS 11.1 for Email Security 릴리스에서는 URL 필터링에서 단축 URL에 대한 지원이 도입되었습니다. CLI 명령 'websecurityadvancedconfig'를 사용하면 단축기 서비스를 보고 구성할 수 있습니다. 이 구성 옵션은 AsyncOS 13.5 for Email Security에서 업데이트되었습니다. 이 릴리스로 업그레이드하면 단축된 모든 URL이 확장됩니다. 단축 URL의 확장을 비활성화할 수 있는 옵션은 없습니다. 따라서 Cisco에서는 URL 방어를 위한 최신 보호 기능을 제공하기 위해 AsyncOS 13.5 for Email Security 이상을 권장합니다. 사용 설명서 또는 온라인 도움말의 "악의적이거나 바람직하지 않은 URL로부터 보호" 장 및 AsyncOS for Cisco Email Security Appliance용 CLI 참조 설명서를 참조하십시오.

참고: 이 문서에서는 AsyncOS 14.2 for Email Security가 제공된 예제 및 스크린샷에 사용됩니다.

참고: Cisco Secure Email에서는 docs.ces.cisco.com에서 심층적인 URL 방어 가이드도 제공합니다.

사전 요구 사항

Cisco Secure Email Gateway 또는 Cloud Gateway에서 URL 필터링을 구성하는 경우, 원하는 기능에 따라 다른 기능도 구성해야 합니다. 다음은 URL 필터링과 함께 활성화되는 몇 가지 일반적인 기능입니다.

- 스팸에 대한 보호를 강화하려면 적용 가능한 메일 정책에 따라 안티스팸 검사 기능을 전역적으로 활성화해야 합니다. 안티스팸은 Cisco IPAS(IronPort Anti-Spam) 또는 Cisco IMS(Intelligent Multi-Scan) 기능으로 간주됩니다.
- 악성코드에 대한 보호를 강화하려면 적용 가능한 메일 정책에 따라 Outbreak Filters 또는

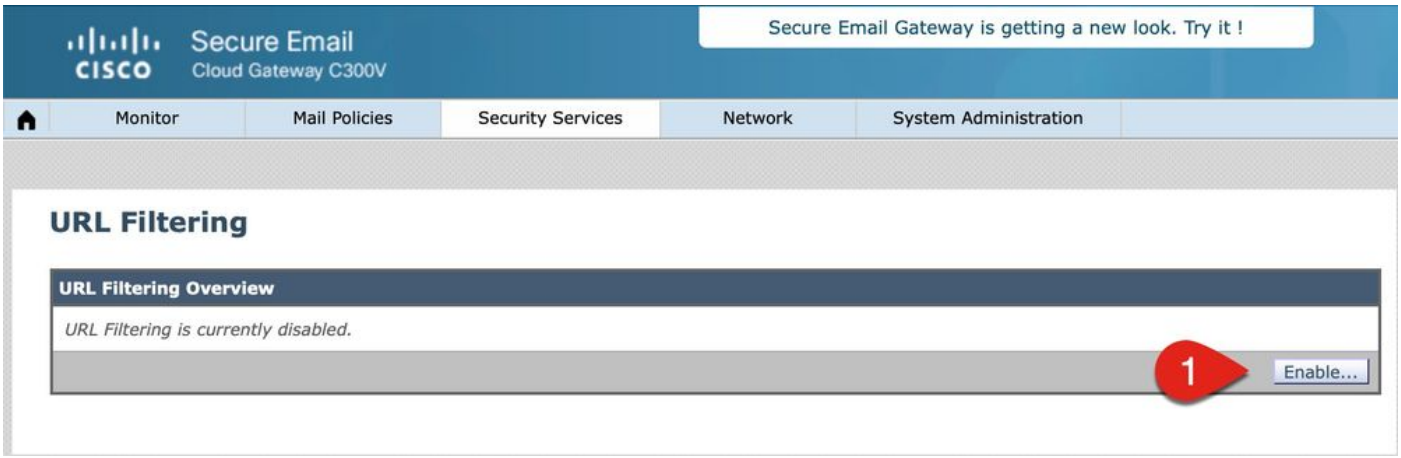
VOF(Virus Outbreak Filters) 기능을 전역적으로 활성화해야 합니다.

- URL 평판을 기반으로 하거나 메시지 및 콘텐츠 필터를 사용하여 허용 가능한 사용 정책을 시행하려면 VOF를 전역적으로 활성화해야 합니다.

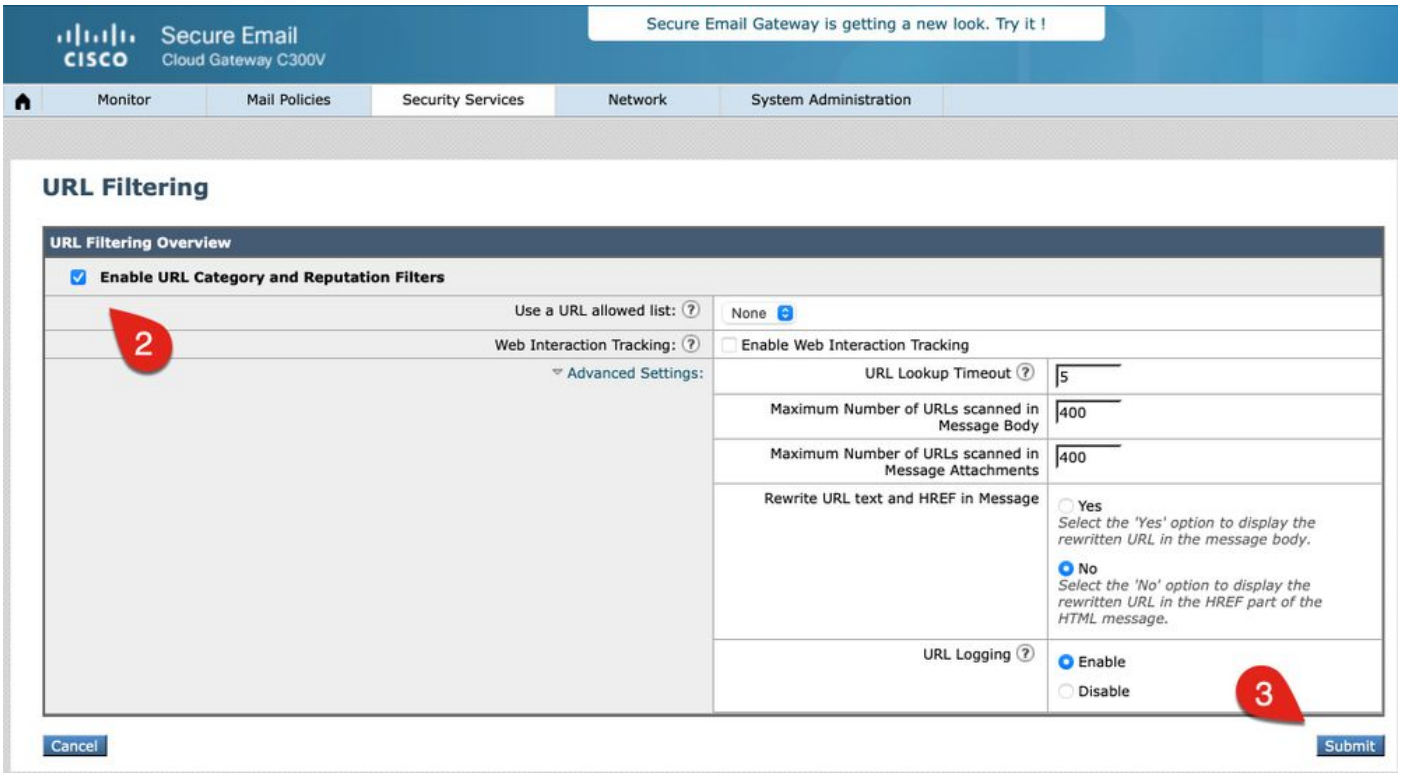
URL 필터링 활성화

먼저 Cisco Secure Email Gateway 또는 Cloud Gateway에서 URL 필터링을 구현하는 기능을 활성화해야 합니다. URL 필터링은 관리자가 GUI 또는 CLI에서 활성화할 수 있습니다.

URL 필터링을 활성화하려면 GUI에서 Security Services(보안 서비스) > URL Filtering(URL 필터링)으로 이동하고 Enable(활성화)을 클릭합니다.



그런 다음 Enable URL Category and Reputation Filters(URL 카테고리 및 평판 필터 활성화)를 클릭합니다. 이 예에는 URL 조회 시간 초과, 검사된 최대 URL 수에 대한 모범 사례 값이 포함되어 있으며, URL 로깅 옵션을 활성화합니다.



참고: 현재 컨피그레이션에 대한 변경 사항을 커밋해야 합니다.

URL 필터링 작업 생성

URL 필터링만 활성화할 경우 메시지 또는 첨부 파일이 있는 메시지 내의 URL에 대해 조치를 취하지 않습니다.

수신 및 발신 메일 정책에 대한 메시지 및 첨부 파일에 포함된 URL이 평가됩니다. URL의 유효한 문자열은 다음 구성 요소의 문자열을 포함하는 것으로 평가됩니다.

- HTTP, HTTPS 또는 WWW
- 도메인 또는 IP 주소
- 콜론(:)이 앞에 오는 포트 번호
- 대문자 또는 소문자

참고: URL 로그 항목은 대부분의 URL에 대해 mail_logs에서 볼 수 있습니다. URL이 mail_logs에 기록되지 않은 경우 메시지 ID(MID)에 대한 메시지 추적을 검토하십시오. 메시지 추적에는 "URL 세부사항" 탭이 포함되어 있지 않습니다.

시스템은 메시지가 스팸인지 확인하기 위해 URL을 평가할 때 로드 관리에 필요한 경우 아웃바운드

메시지보다 인바운드 메시지의 우선 순위를 지정하고 이를 차단합니다.

메시지 본문의 URL 평판 또는 URL 카테고리 또는 첨부 파일이 있는 메시지를 기반으로 메시지에 대한 작업을 수행할 수 있습니다.

예를 들어 Adult(성인) 카테고리의 URL을 포함하는 모든 메시지에 대해 Drop (Final Action)(삭제(최종 작업)) 작업을 적용하려면 선택한 Adult(성인) 카테고리와 함께 URL Category(URL 카테고리) 유형 조건을 추가합니다.

범주를 지정하지 않으면 선택한 작업이 모든 메시지에 적용됩니다.

Trusted(신뢰), Favorite(호의적), Neutral(중립), Questional(의문) 및 Untrusted(신뢰할 수 없음)에 대한 URL 평판 점수 범위는 미리 정의되어 있으며 편집할 수 없습니다. 사용자 지정 범위를 지정할 수 있습니다. 평판 점수가 아직 결정되지 않은 URL에는 "Unknown(알 수 없음)"을 사용합니다.

URL을 빠르게 검사하고 작업을 수행하려면 콘텐츠 필터를 생성하여 메시지에 유효한 URL이 있는 경우 작업이 적용되도록 할 수 있습니다. GUI에서 Mail Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터) > Add Filter(필터 추가)로 이동합니다.

URL과 연결된 작업은 다음과 같습니다.

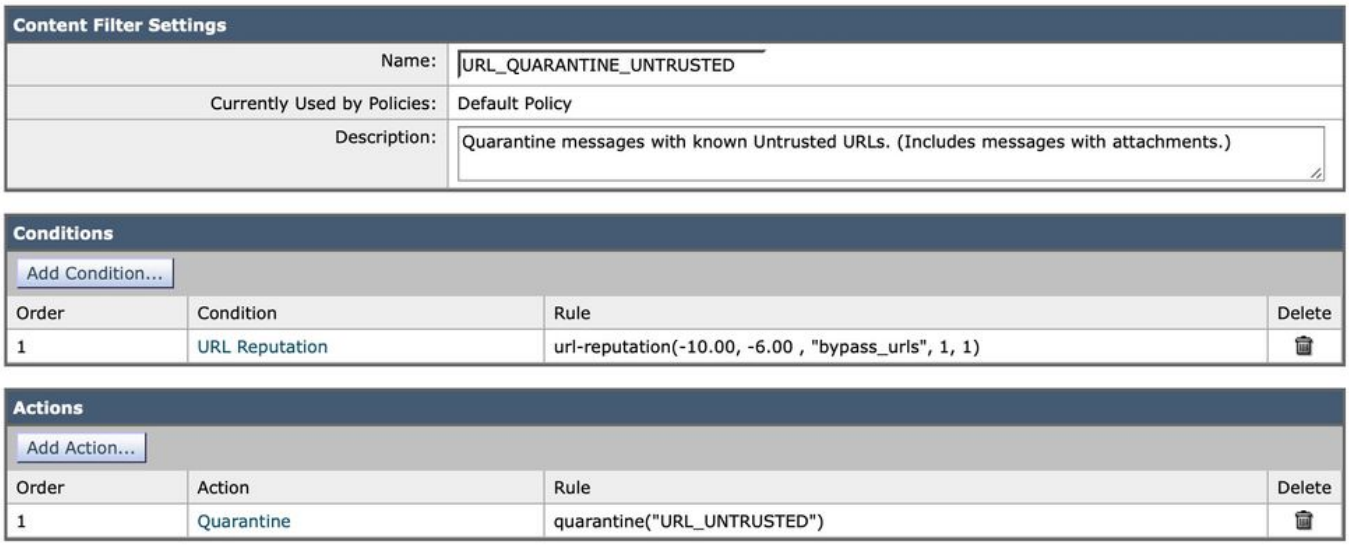
- Defang URL
  - 클릭할 수 없도록 URL이 수정되었지만 메시지 수신자는 여전히 의도한 URL을 읽을 수 있습니다. 추가 문자가 원래 URL에 삽입됩니다.
- Cisco Security Proxy로 이동합니다.
  - 추가 확인을 위해 Cisco Security Proxy를 통과하도록 클릭하면 URL이 재작성됩니다. Cisco Security Proxy 판정에 따라 사용자가 사이트에 액세스할 수 없습니다.
- URL을 텍스트 메시지로 바꾸기
  - 이 옵션을 사용하면 관리자가 메시지 내의 URL을 다시 작성하고 외부에 보내 원격 브라우저 격리를 수행할 수 있습니다.

신뢰할 수 없는 URL

신뢰할 수 없음: 매우 나쁨, 악의적이거나 바람직하지 않은 URL 동작 이는 가장 안전한 권장 차단 목록 임계값입니다. 그러나 URL의 위협 수준이 낮기 때문에 차단되지 않는 메시지가 있을 수 있습니다. 보안보다 제공 우선 순위 지정

권장 조치: 차단. (관리자는 메시지를 완전히 격리하거나 삭제할 수 있습니다.)

다음 예에서는 URL 필터링에 대한 콘텐츠 필터를 통해 신뢰할 수 없는 URL을 탐지할 수 있는 컨텍스트를 제공합니다.



Content Filter Settings

Name:	URL_QUARANTINE_UNTRUSTED
Currently Used by Policies:	Default Policy
Description:	Quarantine messages with known Untrusted URLs. (Includes messages with attachments.)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	quarantine("URL_UNTRUSTED")	

이 콘텐츠 필터를 적용하면 Cisco Secure Email에서 신뢰할 수 없는 평판(-10.00 ~ -6.00)을 가진 URL을 검사하고 메시지를 격리 URL_UNTRUSTED에 배치합니다. 다음은 mail_logs의 예입니다.

<#root>

```
Tue Jul 5 15:01:25 2022 Info: ICID 5 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unite
Tue Jul 5 15:01:25 2022 Info: ICID 5 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:01:25 2022 Info: Start MID 3 ICID 5
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 From: <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host: example.
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 RID 0 To: <end_user>
Tue Jul 5 15:01:25 2022 Info: MID 3 Message-ID '<20220705145935.1835303@ip-127-0-0-1.internal>'
Tue Jul 5 15:01:25 2022 Info: MID 3 Subject "test is sent you a URL => 15504c0618"
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header : 62c45245_jTikQ2lV2NYfmrGzMwQMBd68fxqFFueNmElw
Tue Jul 5 15:01:25 2022 Info: MID 3 ready 3123 bytes from <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:01:25 2022 Info: ICID 5 close
```

Tue Jul 5 15:01:25 2022 Info: MID 3 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matched

Tue Jul 5 15:01:25 2022 Info: MID 3 quarantined to "Policy" (content filter:URL_QUARANTINE_UNTRUSTED)

```
Tue Jul 5 15:01:25 2022 Info: Message finished MID 3 done
```

URL ihaveabadreputation.com은 신뢰할 수 없는 것으로 간주되며 -9.5에서 점수가 매겨집니다. URL 필터링에서 신뢰할 수 없는 URL을 탐지하고 이를 URL_UNTRUSTED로 격리했습니다.

mail_logs의 이전 예는 수신 메일 정책에 대해 URL 필터링의 콘텐츠 필터만 활성화된 경우의 예를

제공합니다. 동일한 메일 정책에 안티스팸과 같은 추가 서비스가 활성화된 경우 다른 서비스는 해당 서비스 및 규칙에서 URL이 탐지되었는지 여부를 나타냅니다. 동일한 URL 예에서 Cisco CASE(Anti-Spam Engine)는 수신 메일 정책에 대해 활성화되며 메시지 본문이 검사되어 스팸 양성으로 확인됩니다. 이는 Anti-Spam이 메일 처리 파이프라인의 첫 번째 서비스이므로 mail_logs에서 먼저 표시됩니다. 콘텐츠 필터는 메일 처리 파이프라인의 나중에 제공됩니다.

<#root>

```
Tue Jul 5 15:19:48 2022 Info: ICID 6 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unite
Tue Jul 5 15:19:48 2022 Info: ICID 6 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:19:48 2022 Info: Start MID 4 ICID 6
Tue Jul 5 15:19:48 2022 Info: MID 4 ICID 6 From: <test@test.com>
Tue Jul 5 15:19:48 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:19:49 2022 Info: MID 4 ICID 6 RID 0 To: <end_user>
Tue Jul 5 15:19:49 2022 Info: MID 4 Message-ID '<20220705151759.1841272@ip-127-0-0-1.internal>'
Tue Jul 5 15:19:49 2022 Info: MID 4 Subject "test is sent you a URL => 646aca13b8"
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Tracker Header : 62c45695_mqwplhpxGDqtgUp/XTLGFKD60hwNKKsghUKA
Tue Jul 5 15:19:49 2022 Info: MID 4 ready 3157 bytes from <test@test.com>
Tue Jul 5 15:19:49 2022 Info: MID 4 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:19:49 2022 Info: ICID 6 close
```

Tue Jul 5 15:19:49 2022 Info: MID 4 interim verdict using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: MID 4 using engine: CASE spam positive

```
Tue Jul 5 15:19:49 2022 Info: ISQ: Tagging MID 4 for quarantine
Tue Jul 5 15:19:49 2022 Info: MID 4 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matche
Tue Jul 5 15:19:49 2022 Info: MID 4 quarantined to "URL_UNTRUSTED" (content filter:URL_QUARANTINE_UNTRU
Tue Jul 5 15:19:49 2022 Info: Message finished MID 4 done
```

CASE 및 IPAS 규칙에 특정 발신자, 도메인 또는 메시지 내용과 일치하는 규칙, 평판 또는 점수가 포함되어 URL 위협만 탐지하는 경우가 있습니다. 이 예에서는 ihaveabadreputation.com이 표시되고 ISQ(Spam Quarantine)에 태그가 지정되었으며 URL_QUARANTINE_UNTRUSTED 콘텐츠 필터에 의해 URL_UNTRUSTED 격리가 지정되었습니다. 메시지가 먼저 URL_UNTRUSTED 격리로 이동합니다. 관리자가 메시지를 쿼런틴에서 해제하거나 URL_UNTRUSTED 쿼런틴의 시간 제한/컨피그레이션 조건이 충족되면 메시지가 ISQ로 이동합니다.

관리자 기본 설정에 따라 콘텐츠 필터에 대한 추가 조건 및 작업을 구성할 수 있습니다.

알 수 없는 URL

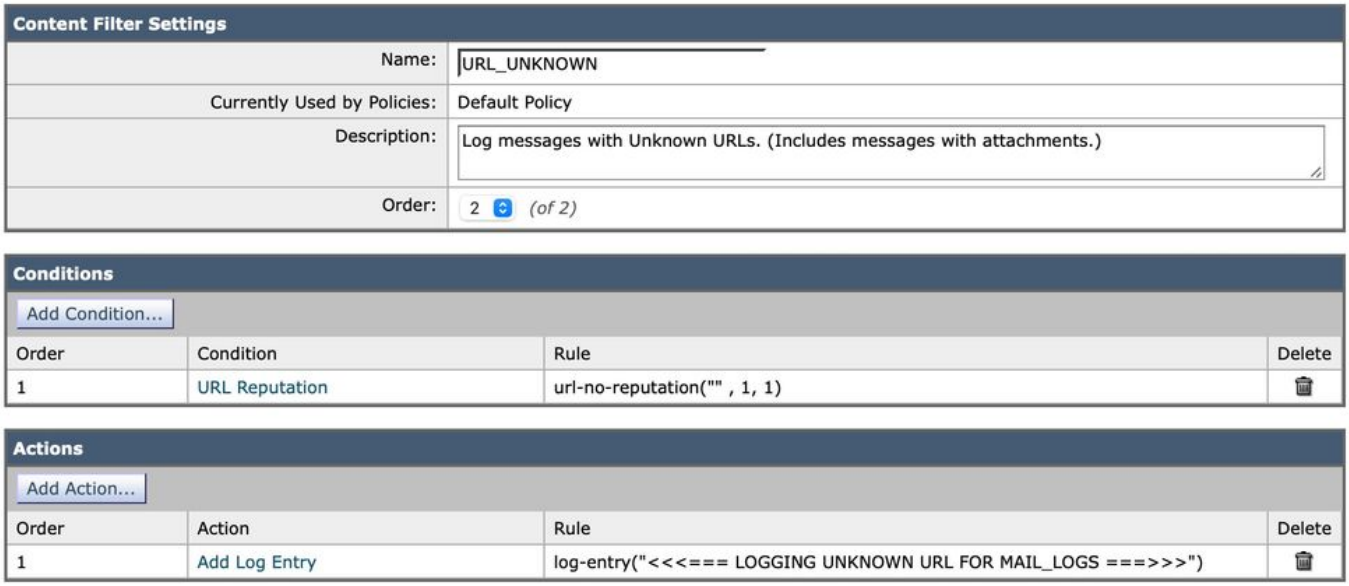
Unknown: 이전에 평가하지 않았거나 위협 레벨 판정을 주장하는 기능을 표시하지 않습니다. URL 평판 서비스에 평판을 설정하기에 충분한 데이터가 없습니다. 이 판정은 URL 평판 정책의 작업에

직접 적합하지 않습니다.

권장 조치: 후속 엔진으로 검사하여 잠재적으로 악의적인 다른 콘텐츠를 확인합니다.

알 수 없는 URL 또는 "평판 없음"은 새 도메인을 포함하는 URL이거나 트래픽이 거의 없거나 전혀 없는 URL일 수 있으며 평가된 평판 및 위협 레벨 판정을 가질 수 없습니다. 도메인 및 출처에 대한 추가 정보가 수집되면 이는 신뢰할 수 없는 것으로 바뀔 수 있습니다. 이러한 URL에 대해서는 로깅할 콘텐츠 필터 또는 알 수 없는 URL 탐지를 포함하는 콘텐츠 필터를 권장합니다. AsyncOS 14.2부터 알 수 없는 URL이 다양한 위협 지표에 대해 트리거된 심층적인 URL 분석을 위해 Talos Intelligence Cloud Service로 전송됩니다. 또한 Unknown URL(s)(알 수 없는 URL)의 메일 로그 항목은 관리자에게 URL Protection(URL 보호)을 통해 MID 및 가능한 교정에 포함된 URL을 알려줍니다. (자세한 내용은 How to configure Cisco Secure Email Account Settings for Microsoft Azure (Microsoft 365) API - Cisco를 참조하십시오.)

다음 예에서는 URL 필터링에 대한 콘텐츠 필터를 사용하여 알 수 없는 URL을 탐지할 수 있는 컨텍스트를 제공합니다.



이 콘텐츠 필터를 적용하면 Cisco Secure Email에서 Unknown 평판 URL을 검색하고 mail_logs에 로그 라인을 작성합니다. 다음은 mail_logs의 예입니다.

<#root>

```
Tue Jul 5 16:51:53 2022 Info: ICID 20 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unit
Tue Jul 5 16:51:53 2022 Info: ICID 20 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 16:51:53 2022 Info: Start MID 16 ICID 20
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 From: <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 RID 0 To: <end_user>
Tue Jul 5 16:51:53 2022 Info: MID 16 Message-ID '<20220705165003.1870404@ip-127-0-0-1.internal>'
Tue Jul 5 16:51:53 2022 Info: MID 16 Subject "test is sent you a URL => e835eadd28"
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
```

```
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Tracker Header : 62c46c29_vrAqZZys2Hqk+BFINVrzdNLLn81kuIf/K6o
Tue Jul 5 16:51:53 2022 Info: MID 16 ready 3208 bytes from <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 matched all recipients for per-recipient policy DEFAULT in the inb
Tue Jul 5 16:51:53 2022 Info: ICID 20 close
Tue Jul 5 16:51:54 2022 Info: MID 16 interim verdict using engine: CASE spam negative
Tue Jul 5 16:51:54 2022 Info: MID 16 using engine: CASE spam negative

Tue Jul 5 16:51:54 2022 Info: MID 16 URL http://mytest.example.com/test_url_2022070503 has reputation no



Tue Jul 5 16:51:54 2022 Info: MID 16 Custom Log Entry: <<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>


Tue Jul 5 16:51:54 2022 Info: MID 16 queued for delivery
Tue Jul 5 16:51:54 2022 Info: Delivery start DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: Message done DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: MID 16 RID [0] Response '2.6.0 <20220705165003.1870404@ip-127-0-0-1.inter
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close
```

URL mytest.example.com/test_url_2022070503은 평판이 없으며 "noscore"로 표시됩니다. URL_UNKNOWN 콘텐츠 필터가 mail_logs에 구성된 대로 로그 라인을 기록했습니다.

Cisco Secure Email Gateway에서 Talos Intelligence Cloud Service로의 폴링 주기가 지나면 URL이 검사되고 신뢰할 수 없는 것으로 확인됩니다. 이는 ECS 로그의 "추적" 레벨에서 확인할 수 있습니다.

```
Tue Jul  5 16:54:42 2022 Debug: ECS: Finish polling
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation service notified.
Tue Jul  5 16:55:42 2022 Debug: ECS: Initiating remediation
Tue Jul  5 16:55:42 2022 Info: ECS: Initiating message remediation:
{'from': ['test@test.com'], 'URL': 'http://mytest.example.com/test_url_2022070503', 'message ID':
'<20220705165003.1870404@ip-172-31-43-120.us-east-2.compute.internal>', 'MID': 16, 'verdict':
'MALICIOUS', 'message UUID': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422'}
Tue Jul  5 16:55:42 2022 Debug: ECS: Unprocessed Remediation Data : [{'url_hash':
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxxyy', 'message_details': '{"mid": 16,
"birth_time": "1657039913", "from_addrs": ["test@test.com"], "recipients": ["[redacted]"],
"delivery_status": 1, "remediation_req_status": 3}', 'created_at': '2022-07-05 16:52:42.04515',
'verdict': '{"url": "http://mytest.example.com/test_url_2022070503", "verdict": "MALICIOUS"}',
'message_uuid': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422', 'message_id':
'<20220705165003.1870404@ip-127-0-0-1.internal>'}]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation records: [
    [
        16,
        "<20220705165003.1870404@ip-127-0-0-1.internal>",
        1657039913,
        "delete",
        3,
        "[{\"url\": \"http://mytest.example.com/test_url_2022070503\", \"conviction_timestamp\":
\"2022-07-05 16:52:42.04515\", \"url_hash\":
\"8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxxyy\"}]",
        [
            "[redacted]"
        ],
        [
            "test@test.com"
        ]
    ]
]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation initiated.
Tue Jul  5 16:55:42 2022 Debug: ECS: Successfully recorded remediation initiation status into datastore.
```

그런 다음 mail_logs에서 교정 자체가 호출되어 완료되면 다음을 수행합니다.

```
Tue Jul 5 16:55:42 2022 Info: Message 16 containing URL 'http://mytest.example.com/test_url_2022070503'
Tue Jul 5 16:55:55 2022 Info: Message 16 was processed due to URL retrospection by Mailbox Remediation
```

관리자는 재량에 따라 알 수 없는 URL에 대한 조치를 고려해야 합니다. 피싱 관련 이메일과 첨부 파일이 증가하는 경우 mail_logs and Content Filters 보고서를 검토하십시오. 또한 관리자는 알 수 없는 URL이 클릭 시 평가를 위해 Cisco 보안 프록시 서비스로 리디렉션되도록 구성할 수 있습니다. 이 예에서는 URL_UNKNOWN 콘텐츠 필터 내에서 Add Action(작업 추가) > URL Reputation(URL 평판)으로 이동합니다.

URL Reputation

Help

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBRS) or using information from the External Threat Feed engine.

Matching Condition

- (•) URL Reputation
  - ( ) Untrusted (-10.0 to -6.0)
  - ( ) Questionable (-5.9 to -3.1)
  - ( ) Neutral (-3.0 to 0.0)
  - ( ) Favorable (0.1 to 5.9)
  - ( ) Trusted (6.0 to 10.0)
  - ( ) Custom Range (min to max)
  - (•) Unknown
- ( ) External Threat Feeds

This option is currently unavailable because no threat feed sources have been configured. To create one, go to Mail Policies > External Threat Feeds Manager.

Use a URL allowed list: None

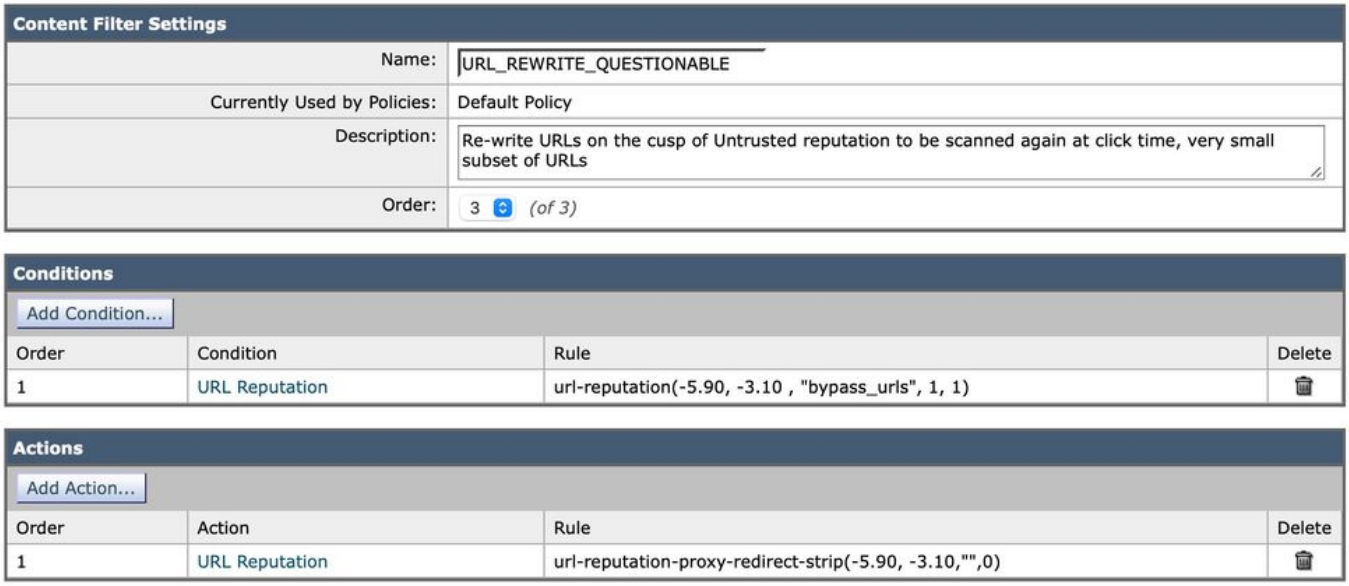
Check URLs within

- ( ) Message Body and Subject
- ( ) Attachments
- (•) All (Message Body, Subject and Attachments)

Action on URL within the message body and subject:

비율이 낮고 상대적으로 안전합니다. 차단되지 않은 판정은 보안보다 전달의 우선 순위를 지정하므로 위험한 URL이 포함된 메시지가 표시될 수 있습니다.
권장 조치: 후속 엔진으로 스캔하고 검토 후 차단

알 수 없는 URL에 구성했듯이 관리자는 의심스러운 URL을 Cisco 보안 프록시에 보내거나 작업을 통해 URL을 완전히 방어하는 것이 유익하다고 생각할 수 있습니다.



중립 URL

Neutral: 긍정 또는 부정 동작이 없는 URL. 그러나, 그것은 평가되었습니다. 즉, URL에는 현재 알려진 위험이 없습니다. 따라서, 이것은 평판 판결의 대부분이다.
권장 조치: 후속 엔진으로 검사하여 잠재적으로 악의적인 다른 콘텐츠를 확인합니다.

관리자는 음수 점수의 Neutral URL을 위협으로 볼 수 있습니다. 재량에 따라 메시지의 수 및 Neutral URL의 발생을 평가합니다. 알 수 없는 URL 및 의심스러운 URL을 업데이트하여 Cisco Security Proxy에 URL을 보내는 작업을 활용하는 방법과 마찬가지로, Neutral URL 또는 Neutral의 음수 부분 집합을 포함하는 Custom Range를 고려할 수 있습니다. 다음 예에서는 이 인바운드 콘텐츠 필터를 구현하여 중립 URL을 검사하는 방법을 보여 줍니다.

Content Filter Settings

Name:	URL_NEUTRAL
Currently Used by Policies:	*No policies currently use this rule.*
Description:	Send questionable Neutral URLs to be scanned again at click time. (Includes messages with attachments.)
Order:	4 *(of 4)*

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-3.00, -0.50 , "", 1, 1)	

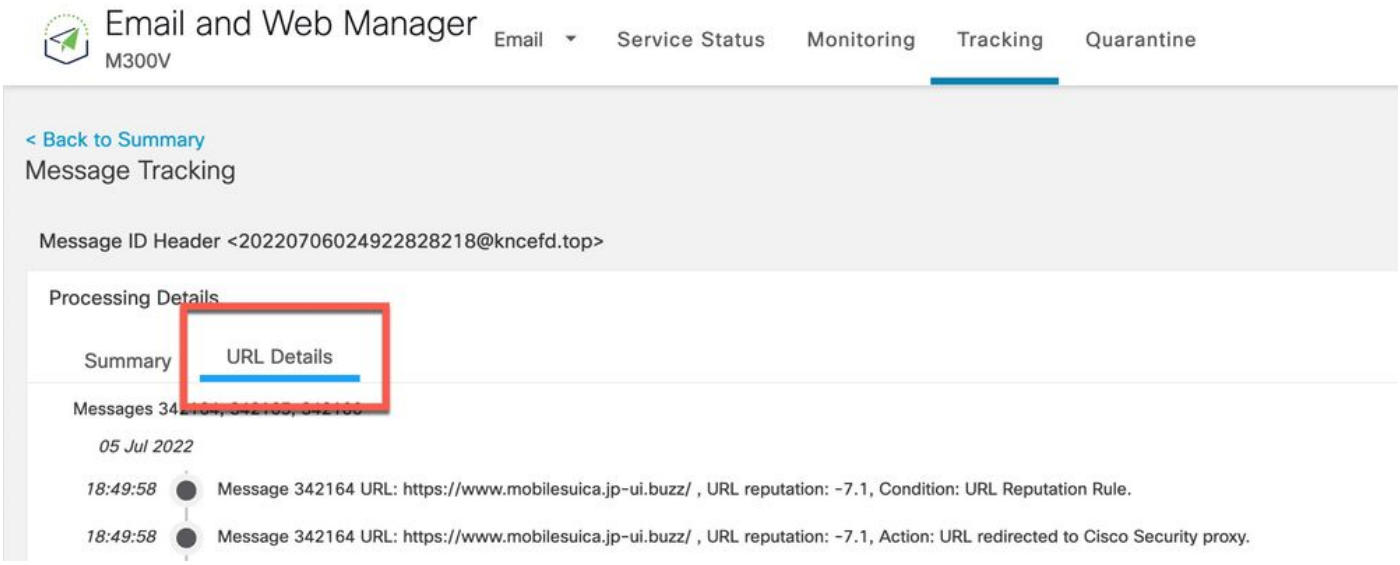
Actions

Add Action...

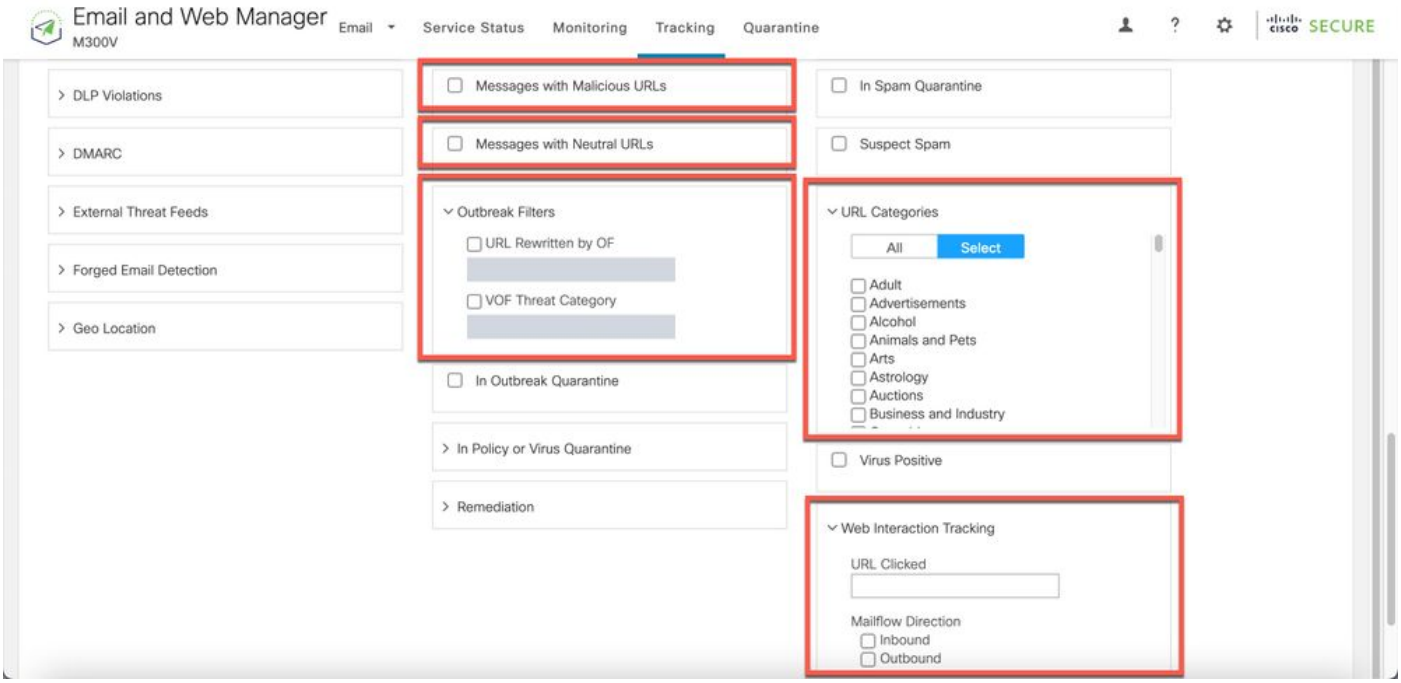
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

메시지 추적

MID가 있는 연결된 URL에 대한 메시지 추적 옵션을 검토합니다. URL이 mail_logs에 기록되지 않는 경우가 있으며, 메시지 추적 세부 정보에서 URL을 찾을 수 있습니다. 예를 들면 다음과 같습니다.



메시지 추적은 또한 URL 방어 및 상호 작용이 있는 메시지에 대한 고급 검색 옵션을 제공합니다.



분류되지 않은 URL 및 잘못 분류된 URL 보고

URL은 때로는 평판 또는 분류 없이 보고될 수 있습니다. 잘못 분류된 URL도 있습니다. 이러한 URL 탐지를 보고하려면 Talos의 Reputation Center Support(평판 센터 지원) 페이지에서 Cisco Talos의 Web Categorization Requests(웹 분류 요청)를 방문하십시오.

URL을 보고한 후에는 내 티켓 페이지를 참조하십시오.

악의적인 URL 및 마케팅 메시지가 안티스팸 또는 Outbreak Filter로 검색되지 않음

이는 안티스팸 및 Outbreak Filter가 판정을 위해 사용하는 여러 조건 중 사이트 평판 및 범주가 두 가지 기준이기 때문에 발생할 수 있습니다. 이러한 필터의 민감도를 높이려면 재작성 또는 URL을 텍스트로 교체, 격리 또는 메시지 삭제와 같은 작업을 수행하는 데 필요한 임계값을 낮춥니다.

또는 URL 평판 점수를 기반으로 콘텐츠 또는 메시지 필터를 만들 수 있습니다.

부록

단축 URL에 대한 URL 필터링 지원 활성화

참고: 이 섹션은 Email Security용 AsyncOS 11.1~13.0에만 적용됩니다.

단축 URL에 대한 URL 필터링 지원은 CLI에서만 수행할 수 있으며 websecurityadvancedconfig 명령은 다음과 같습니다.

```
<#root>

myesa.local>

websecurityadvancedconfig


...

Do you want to enable URL filtering for shortened URLs? [N]>

Y


For shortened URL support to work, please ensure that ESA is able to connect to following domains:
bit.ly, tinyurl.com, ow.ly, tumblr.com, ff.im, youtu.be, tl.gd, plurk.com, url4.eu, j.mp, goo.gl, yfrog
```

URL 필터링 컨피그레이션 모범 사례를 위해 이 기능을 활성화하는 것이 좋습니다. 활성화되면 메일 로그는 메시지 내에서 단축된 URL이 사용될 때마다 반영됩니다.

```
Mon Aug 27 14:56:49 2018 Info: MID 1810 having URL: http://bit.ly/2tztQUi has been expanded to https://
```

이 문서에서 설명한 대로 URL 필터링이 활성화되면 mail_logs 예제에서 bit.ly 링크가 기록되고 확장되는 원래 링크도 기록됩니다.

추가 정보

Cisco Secure Email Gateway 설명서

- 릴리스 정보
- 사용 설명서
- CLI 참조 가이드
- Cisco Secure Email Gateway용 API 프로그래밍 가이드
- Cisco Secure Email Gateway에서 사용되는 오픈 소스
- Cisco Content Security Virtual Appliance 설치 설명서(vESA 포함)

Secure Email Cloud Gateway 설명서

- 릴리스 정보
- 사용 설명서

Cisco Secure Email and Web Manager 설명서

- 릴리스 정보 및 호환성 매트릭스
- 사용 설명서
- Cisco Secure Email and Web Manager용 API 프로그래밍 가이드
- Cisco Content Security Virtual Appliance 설치 설명서(vSMA 포함)

Cisco Secure Product 문서

- Cisco Secure 포트폴리오 명명 아키텍처

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.