Cisco AsyncOS API for Email - 시작 가이드

릴리스 1.0
게시: 2015년 5월 28일

목차

Cisco AsyncOS API for Email 개요

Cisco AsyncOS API for Email(AsyncOS API)은 REST(Representational StateTransfer) 기반의 작업 모음이며 Email Security Appliance 보고서 및 보고서 카운터에 대한 안전하고 인증된 액세스를 제공합니다. 이 API를 사용하여 ESA(Email Security Appliance) 보고 데이터를 검색할 수 있습니다.

Cisco Systems, Inc.
www.cisco.com

AsyncOS API 사용을 위한 사전 요구 사항

AsyncOS API를 사용하려면 다음 항목이 필요합니다.

- Cisco AsyncOS 9.0 for Email 이상을 실행하는 ESA
- 다음에 관한 지식:
  - API 트랜잭션에 사용하는 프로토콜인 HTTP
  - TLS를 통한 보안 통신
  - API에서 리소스 표현을 구성하는 데 사용하는 JSON(JavaScript Object Notation)
- HTTP 또는 HTTPS를 사용하여 AsyncOS API 요청을 시작하거나 응답을 수신하는 클라이언트 또는 프로그래밍 라이브러리(예: cURL). 클라이언트 또는 프로그래밍 라이브러리는 API 응답을 해석하기 위해 JSON을 지원해야 합니다.
- AsyncOS API 액세스 권한. 권한 부여, 3페이지를 참조하십시오.
- 웹 인터페이스 또는 CLI를 사용하여 활성화된 AsyncOS API. AsyncOS API 활성화, 2페이지를 참조하십시오.

AsyncOS API 활성화

시작하기 전에

웹 인터페이스의 IP Interfaces(IP 인터페이스) 페이지 또는 CLI의 `interfaceconfig` 명령에 대한 액세스 권한이 있어야 합니다. 관리자와 운영자만 이 페이지 또는 명령에 액세스할 수 있습니다.

절차

1단계 웹 인터페이스에 로그인합니다.

2단계 **Network(네트워크) > IP Interfaces(IP 인터페이스)**를 클릭합니다.

3단계 Management(관리) 인터페이스를 수정합니다.

참고 어떤 IP 인터페이스에서도 AsyncOS API를 활성화할 수 있습니다. 그러나 Management(관리) 인터페이스에서 AsyncOS API를 활성화하는 것이 좋습니다.

4단계 AsyncOS API (Monitoring)(모니터링) 섹션에서 요구 사항에 따라 HTTP, HTTPS 또는 둘 다와 사용할 포트를 선택합니다.

참고 AsyncOS API는 HTTP/1.0을 사용하여 통신합니다.

HTTPS를 선택한 상태에서 보안 통신에 자체 인증서를 사용하려는 경우 AsyncOS API와의 보안 통신, 3페이지를 참조하십시오.

참고 항상 프로덕션 환경에서 HTTPS를 사용하는 것이 좋습니다. HTTP는 API 문제 해결 및 테스트에만 사용하십시오.

5단계 변경 사항을 제출 및 커밋합니다.

CLI에서 `interfaceconfig` 명령을 사용하여 AsyncOS API를 활성화할 수도 있습니다.

AsyncOS API와의 보안 통신

자체 인증서를 사용하여 보안 HTTP를 통해 AsyncOS API와 통신할 수 있습니다.

참고 이미 HTTPS를 통해 웹 인터페이스를 실행하고 있거나 보안 통신에 자체 인증서를 사용하고 있는 경우 이 절차를 수행하지 마십시오. AsyncOS API에서는 동일한 인증서를 HTTPS를 통한 통신에서 웹 인터페이스로 사용합니다.

절차

1단계 웹 인터페이스에서 **Network(네트워크) > Certificates(인증서)** 페이지를 사용하거나 CLI에서 `certconfig` 명령을 사용하여 인증서를 설정합니다. 자세한 내용은 *Cisco AsyncOS for Email 사용 설명서* 또는 온라인 도움말을 참조하십시오.

2단계 웹 인터페이스에서 **Network(네트워크) > IP Interfaces(IP 인터페이스)** 페이지를 사용하거나 CLI에서 `interfaceconfig` 명령을 사용하여 IP 인터페이스에서 사용하는 HTTPS 인증서를 해당 인증서로 변경합니다. 자세한 내용은 *Cisco AsyncOS for Email 사용 설명서* 또는 온라인 도움말을 참조하십시오.

3단계 변경 사항을 제출 및 커밋합니다.

AsyncOS API 인증 및 권한 부여

권한 부여

다음 역할의 ESA 사용자는 AsyncOS API에 액세스할 수 있습니다.

- Administrator
- Read-Only Operator
- 운영자
- 게스트

참고 중앙 집중식 인증 시스템(LDAP 또는 RADIUS 디렉토리)의 사용자는 Cisco AsyncOS API for Email에 액세스할 수 없습니다. LDAP 또는 RADIUS 디렉토리 사용자가 API 액세스를 시도할 경우 API는 401 오류 메시지를 보냅니다.

인증

API 사용자는 모든 API 요청에 base64 인코딩 형식으로 ESA 사용자 이름과 비밀번호를 제출해야 합니다. 요청의 Authorization 헤더에 유효한 인증서가 없을 경우 API는 401 오류 메시지를 보냅니다.

인증서를 base64 인코딩 형식으로 변환하는 데 어떤 base64 라이브러리도 사용할 수 있습니다. 다음 표에는 base64 인코딩 인증서의 예가 나와 있습니다.

항목	값
Username	`administrator`
Password	`Password$123`
인증서	`administrator:Password$123`
Base64 인코딩 인증서	`YWRtaW5pc3RyYXRvcjpQYXNzd29yZCQxMjM=`

참고 인코딩된 인증서는 헤더 내에 한 줄에 있어야 합니다.

AsyncOS API 요청 및 응답

AsyncOS API 요청

API에 대한 요청은 다음과 같은 특성이 있습니다.

- 요청은 HTTP 또는 HTTPS를 통해 전송됩니다.
- 각 요청은 `https://{appliance}:{port}/api/v1.0/{resource}?{resource_attributes}` 형식의 유효한 URI를 포함해야 합니다. 여기서
  - `{appliance}:{port}`는 어플라이언스의 FQDN 또는 IP 주소이고 어플라이언스가 수신하는 TCP 포트 번호입니다.
  - `{resource}`는 액세스하려는 리소스(예: 보고서 또는 카운터)입니다.
  - `{resource_attributes}`는 리소스에 대해 지원되는 특성(예: 기간, 최대값 등)입니다.
- 각 요청은 base64 인코딩 형식의 유효한 권한 부여 헤더를 포함해야 합니다.
- 각 요청에서는 Accept가 `application/json`으로 설정되어야 합니다.
- (사용자 자체 인증서를 사용하여) HTTPS를 통해 보내진 요청은 사용자의 CA 인증서를 포함해야 합니다. 예를 들어 cURL의 경우 다음과 같이 API 요청에서 CA 인증서를 지정할 수 있습니다.

```
curl --cacert <ca_cert.crt> -u "username:password"
https://<fqdn>:<port>/api/v1.0/{resource}?{resource_attributes}
```

참고 API 요청은 대/소문자를 구분하며 본 가이드에 표시된 대로 입력해야 합니다.

요청의 구조

다음 표에는 AsyncOS API에서 사용할 수 있는 요청 작업의 유형이 나와 있습니다.

요청 유형	설명
GET	지정된 리소스에 데이터를 요청합니다.

다음 표에는 요청의 필수 헤더가 나와 있습니다.

헤더	값	설명
Host	`{appliance}:{port}`	어플라이언스의 도메인 이름 또는 IP 주소 및 어플라이언스가 수신하는 TCP 포트 번호
Accept	• `application/json` • `*/*`	이 클라이언트에서 허용하려는 미디어 유형을 리소스 버전을 포함하여 서버에 표시합니다.
Authorization	Basic{base64-encoded(username:password)}	이 요청을 수행하는 허가받은 사용자를 나타냅니다.

AsyncOS API 응답

응답의 주요 구성 요소

구성 요소		값	설명
상태 코드 및 이유		HTTP 응답 코드, 6페이지를 참조하십시오.	HTTP 응답 코드와 이유
메시지 헤더	Content-Type	• `application/json`	메시지 본문의 형식을 나타냅니다.
	Content-Length	해당 없음	응답 본문의 길이(옥텟)
	Connection	`close`	연결을 위해 선택할 옵션

메시지 본문		해당 없음	메시지 본문의 형식은 Content-Type 헤더에 정의됩니다. 그 다음에는 메시지 본문의 구성 요소가 옵니다.
			1. URI. API 요청에 지정한 URI입니다.
			예
			`"uri":"/api/v1.0/health/"`
			2. 링크 또는 데이터
			– 링크. 계층 구조상 다음 레벨 리소스의 목록입니다.
			예
			`"links": {"percentage_ram_utilization": "Percentage...}`
			– 데이터. 지정된 URI를 기반으로 API에서 제공하는 보고 데이터
			예
			`"data": {"percentage_diskio": 10}`
			3. (오류 이벤트만 해당) 오류. 이 구성 요소는 message, code, explanation의 3개 하위 구성 요소로 이루어집니다.
			예
			`"error": {"message": "Unexpected attribute - starts_with.", "code": "404", "explanation": "404 = Nothing matches the given URI."}`
			참고 메시지 본문에 빈 괄호({})가 있을 경우 API에서 쿼리와 매치하는 레코드를 찾지 못했음을 의미합니다.

HTTP 응답 코드

다음은 AsyncOS API에서 반환하는 HTTP 응답 코드의 목록입니다.

- 200
- 400
- 401
- 404

- 406
- 413
- 414
- 500
- 501
- 505

이 HTTP 응답 코드에 대한 설명은 다음 RFC를 참조하십시오.

- RFC1945
- RFC7231

AsyncOS API 기능

AsyncOS API를 사용하여 다음 작업을 수행할 수 있습니다.

- 어플라이언스의 현재 상태 매개변수 검색, 7페이지
- Email Security Appliance 통계 보고서 검색, 8페이지
- 인라인 도움말 Cisco AsyncOS API for Email 액세스, 12페이지

어플라이언스의 현재 상태 매개변수 검색

어플라이언스의 상태를 평가하기 위해 RAM 사용률, 큐 사용률, 작업 큐의 메시지 등 어플라이언스의 현재 키 상태 매개변수를 검색할 수 있습니다.

설명	ESA의 주요 상태 매개변수를 검색합니다.
개요	`GET /api/v1.0/health` `GET /api/v1.0/health/{parameter}`
요청 헤더	Host, Accept, Authorization
응답 헤더	Content-Type, Content-Length, Connection

예

샘플 요청

```
GET /api/v1.0/health HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

샘플 응답

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Wed, 02 Jul 2014 05:07:50 GMT
Content-type: application/json
Content-Length: 246
Connection: close
```

```
{
    "data":{
        "percentage_ram_utilization":10,
        "percentage_diskio":20,
        "resource_conservation":3,
        "messages_in_workqueue":189,
        "messages_in_pvo_quarantines":12,
        "percentage_swap_utilization":2.0,
        "percentage_queue_utilization":5.0,
        "percentage_cpu_load":12
    },
    "uri":"/api/v1.0/health/"
}
```


참고 이 상태 매개변수에 대한 자세한 내용은 URI `https://{appliance}:{port}/api/v1.0/health/help`를 사용하여 API 인라인 도움말을 참조하십시오. 인라인 도움말 Cisco AsyncOS API for Email 액세스, 12페이지를 참조하십시오.

Email Security Appliance 통계 보고서 검색

어플라이언스에서 수신 메일 요약, 바이러스 유형 등 다양한 통계 보고서를 검색할 수 있습니다. 통계 보고서는 3가지 유형으로 분류할 수 있습니다.

- **Simple Report(간략 보고서)**. 이 보고서 범주에서는 지정된 기간에 일어난 어플라이언스의 다양한 이벤트(예: 인증 시도 실패 횟수, 트리거한 콘텐츠 필터 수 등)를 카운트합니다. 예를 들어 `mail_authentication_summary` 및 `mail_dlp_outgoing_traffic_summary`가 있습니다.
- **Top-N Report(상위 N 보고서)**. 이 보고서 범주에서는 지정된 기간에서 어떤 엔티티(IP 주소, 도메인 이름 등)에 대해 어플라이언스에서 발생한 다양한 이벤트를 카운트하며 상위 N개 이벤트를 나열합니다. 여기서 N은 사용자가 지정하는 값입니다. 예를 들어 `mail_content_filter_incoming` 및 `mail_dmarc_incoming_traffic_summary`가 있습니다.
- **Query-based Report(쿼리 기반 보고서)**. 이 보고서 범주에서는 지정된 기간에 사용자 지정 엔티티(IP 주소, 도메인 이름 등)에 대해 어플라이언스에서 발생한 다양한 이벤트를 카운트합니다. 예를 들어 `mail_authentication_incoming_domain` 및 `mail_content_filter_outgoing`이 있습니다.

각 범주에 속하는 보고서의 목록은 통계 보고서, 14페이지를 참조하십시오.

설명	ESA의 다양한 통계 보고서를 검색합니다.
개요	`GET /api/v1.0/stats/report?resource_attribute` `GET /api/v1.0/stats/report/counter?resource_attribute`

지원되는 리소스 특성	**간략 보고서**	• `time_range`. 지정된 기간의 보고서를 검색할 때 이 특성을 사용합니다. 이 특성은 다음 값을 가질 수 있습니다. – `1h` - 지난 1시간의 보고서를 종합합니다. – `1d` - 지난 1일의 보고서를 종합합니다. – `duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD` - 지정된 기간의 보고서를 종합합니다. `TZD`에서 지원되는 값은 `Z`, `+hh:mm` 또는 `-hh:mm`입니다.
	상위 N 보고서	• `time_range`. 지정된 기간의 보고서를 검색할 때 이 특성을 사용합니다. 이 특성은 다음 값을 가질 수 있습니다. – `1h` - 지난 1시간의 보고서를 종합합니다. – `1d` - 지난 1일의 보고서를 종합합니다. – `duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD` - 지정된 기간의 보고서를 종합합니다. `TZD`에서 지원되는 값은 `Z`, `+hh:mm` 또는 `-hh:mm`입니다. • `max=n`. 보고서에서 반환하는 값의 수를 제한할 때 이 특성을 사용합니다. `n`은 보고서에서 반환할 결과의 수이며 1 ~ 1000 범위의 값을 사용할 수 있습니다.
	쿼리 기반 보고서	• `time_range`. 지정된 기간의 보고서를 검색할 때 이 특성을 사용합니다. 이 특성은 다음 값을 가질 수 있습니다. – `1h` - 지난 1시간의 보고서를 종합합니다. – `1d` - 지난 1일의 보고서를 종합합니다. – `duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD` - 지정된 기간의 보고서를 종합합니다. `TZD`에서 지원되는 값은 `Z`, `+hh:mm` 또는 `-hh:mm`입니다. • `entity=value`. 이메일 주소, IP 주소 등 지정된 엔티티를 기반으로 보고서를 검색할 때 이 특성을 사용합니다. 지정된 텍스트와 정확하게 매치할지 아니면 지정된 텍스트로 시작하는 항목을 찾을지(예: starts with "ex"는 "example.com"과 매치) 선택할 수 있습니다. **참고** 이 특성의 정의는 보고서 유형에 따라 다릅니다. 이 특성에 사용할 수 있는 값에 대해서는 통계 보고서, 14페이지를 참조하십시오. 지정된 텍스트로 시작하는 항목을 검색하려면 이 특성을 `starts_with` 특성과 함께 사용해야 합니다(예: `entity=us&starts_with=true`). • `starts_with=value`. 지정된 엔티티 값으로 시작하는 항목을 검색하려면 이 특성을 사용합니다. 이 특성은 `entity` 특성과 함께 사용해야 하며 `value`는 `true`로 설정되어야 합니다(예: `entity=us&starts_with=true`). • `max=n`. 보고서에서 반환하는 값의 수를 제한할 때 이 특성을 사용합니다. `n`은 보고서에서 반환할 결과의 수이며 1 ~ 1000 범위의 값을 사용할 수 있습니다. **참고** `entity` 특성과 `max=n` 특성을 동일한 요청에 사용할 수 없습니다.

요청 헤더	Host, Accept, Authorization
응답 헤더	Content-Type, Content-Length, Connection

참고 여러 특성을 사용하려면 AND(&) 연산자를 사용합니다(예: `https://{appliance}:{port}/api/v1.0/stats/report/counter?attribute1&attribute2`).

참고 통계 보고서 및 카운터에 대한 자세한 내용은 API 인라인 도움말을 참조하십시오. 인라인 도움말 Cisco AsyncOS API for Email 액세스, 12페이지를 참조하십시오.

예

- 간략 보고서 유형, 10페이지
- 상위 N 보고서 유형, 11페이지
- 쿼리 기반 보고서 유형, 11페이지

간략 보고서 유형

다음 예에서는 지난 1일의 종합 Incoming Mail Summary(수신 메일 요약) 보고서를 검색하는 방법을 보여줍니다.

샘플 요청

```
GET /api/v1.0/stats/mail_incoming_traffic_summary?1d HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

샘플 응답

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Tue, 15 Jul 2014 08:26:46 GMT
Content-type: application/json
Content-Length: 461
Connection: close

{
    "data":{
        "verif_decrypt_success":0,
        "detected_virus":1396438,
        "threat_content_filter":106728,
        "blocked_invalid_recipient":209054,
        "verif_decrypt_fail":0,
        "marketing_mail":0,
        "detected_amp":0,
        "ims_spam_increment_over_case":0,
        "total_recipients":827216461,
        "detected_spam":1265606,
        "total_clean_recipients":1977205,
        "blocked_dmarc":0,
        "malicious_url":14006,
        "total_threat_recipients":825239256,
```

```
        "blocked_reputation":822261430
    },
    "uri":"/api/v1.0/stats/mail_incoming_traffic_summary?1d"
}
```

상위 N 보고서 유형

다음 예에서는 지정된 기간의 대용량 메일 중에서 상위 5개 제목을 검색하는 방법을 보여줍니다.

샘플 요청

```
GET
/api/v1.0/stats/mail_subject_stats?duration=2014-04-23T00:00-00:00/2014-10-21T00:00-00:00&
max=5 HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

샘플 응답

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Tue, 15 Jul 2014 08:26:46 GMT
Content-type: application/json
Content-Length: 182
Connection: close

{
    "data":{
        "num_msgs":{
            "Buying judgments":44584,
            "Additional Income":39691,
            "Why pay more?":46044,
            "Message contains":50460,
            "Off shore":56954
        }
    },

"uri":"/api/v1.0/stats/mail_subject_stats?duration=2014-04-23T00:00-00:00/2014-10-21T00:00
-00:00&max=5"
}
```

쿼리 기반 보고서 유형

다음 예에서는 지정된 기간에 "2001::6"으로 시작하는 IP 주소에 대한 종합 Outgoing Sender(발신자) 보고서를 검색하는 방법을 보여줍니다.

샘플 요청

```
GET
/api/v1.0/stats/mail_sender_ip_hostname_detail?duration=2014-04-23T00:00-00:00/2014-10-21T
00:00-00:00&entity=2001::63&starts_with=true HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

샘플 응답

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Thu, 04 Sep 2014 09:27:58 GMT
```

```
Content-type: application/json
Content-Length: 633
Connection: close

{
    "data":{
        "2001::63":{
            "detected_virus":2,
            "threat_content_filter":0,
            "total_dlp_incidents":0,
            "total_clean_recipients":4372,
            "total_recipients_processed":4374,
            "detected_spam":0,
            "total_threat_recipients":2
        }
        "2001::6":{
            "detected_virus":2,
            "threat_content_filter":0,
            "total_dlp_incidents":0,
            "total_clean_recipients":1232,
            "total_recipients_processed":1234,
            "detected_spam":0,
            "total_threat_recipients":2
        }
    },
"uri":"/api/v1.0/stats/mail_sender_ip_hostname_detail?duration=2014-04-23T00:00-00:00/2014
-10-21T00:00-00:00&entity=2001::6&starts_with=true"
}
```

인라인 도움말 Cisco AsyncOS API for Email 액세스

AsyncOS API에서는 지원되는 모든 보고서 및 카운터에 대한 종합 인라인 도움말을 제공합니다. URI의 끝에 `/help`를 추가하여 보고서 또는 카운터에 대한 인라인 도움말에 액세스할 수 있습니다.

몇 가지 예를 들면 다음과 같습니다.

- `GET /api/v1.0/stats/help` 통계 보고서와 그 설명의 목록을 검색할 수 있습니다.
- `GET /api/v1.0/health/help` 어플라이언스의 주요 상태 매개변수와 그 설명의 목록을 검색할 수 있습니다.
- `GET /api/v1.0/stats/mail_incoming_traffic_summary/help` Incoming Mail Summary(수신 메일 요약) 보고서의 설명, 이 보고서에서 지원되는 카운터 및 그에 대한 설명, 보고서 범주를 검색할 수 있습니다.
- `GET /api/v1.0/stats/mail_incoming_traffic_summary/detected_virus/help` Incoming Mail Summary(수신 메일 요약) 보고서의 "`detected_virus`" 카운터에 대한 설명을 검색할 수 있습니다.

AsyncOS API 문제 해결

API 로그

System Administration(시스템 관리) > Log Subscriptions(로그 구독)을 사용하여 API 로그를 구독합니다. 자세한 내용은 *Cisco AsyncOS for Email 사용 설명서* 또는 온라인 도움말을 참조하십시오.

다음은 API 로그에 로깅되는 이벤트 중 일부입니다.

- API 시작 또는 중지
- (응답 후) API와의 연결 실패 또는 종료
- 인증 성공 또는 실패
- 요청에 오류 있음
- AsyncOS API에 네트워크 구성 변경 사항을 알리는 중 오류 발생

알림

AsyncOS API와 관련된 알림을 보낼 수 있도록 어플라이언스를 구성해야 합니다. 다음과 같은 상황에서 알림을 받습니다.

알림 설명	유형	심각도
오류 때문에 API를 재시작했습니다.	시스템	경고
웹 인터페이스 또는 CLI에서 네트워크 구성 또는 인증서를 변경했으나 API에 전달되지 않았습니다. 네트워크 구성 또는 인증서 변경 사항이 AsyncOS API에 전달되지 않은 것에 대한 알림, 13페이지를 참조하십시오.	시스템	중대

네트워크 구성 또는 인증서 변경 사항이 AsyncOS API에 전달되지 않은 것에 대한 알림

문제 웹 인터페이스 또는 CLI에서 네트워크 구성 또는 인증서를 변경했으나 API에 전달되지 않았다는 내용의 중대 심각도의 알림을 받습니다.

솔루션 다음과 같이 해보십시오.

- 어플라이언스를 재시작합니다.
- 문제가 계속되면 TAC에 문의하십시오.

cURL 사용 중 인증서 오류

문제 일부 운영 체제(예: Unix, Ubantu, Mac OS X 등)에서 API와의 보안 통신에 HTTPS와 자체 인증서를 사용하는 경우 cURL을 사용하여 API 리소스를 요청할 때 인증서 오류가 발생할 수 있습니다. 몇 가지 예를 들면 다음과 같습니다.

- `curl: (60) SSL certificate problem: Invalid certificate chain`
- `curl: (77) error setting certificate verify locations`

솔루션 cURL 설명서(http://curl.haxx.se/)를 참조하십시오.

AsyncOS API 참조

통계 보고서

간략 보고서

mail_authentication_summary

설명

수신 메일에 대한 SMTP 인증 통계 요약

웹 인터페이스의 보고서

Monitor(모니터링) > Inbound SMTP Authentication(인바운드 SMTP 인증) > Received Connections(수신 연결)

카운터	설명
received_conn_cert_success	클라이언트 인증서로 인증하여 성공한 총 수신 연결 수
received_auth	수신하고 인증한 총 수신자 수
received_total	수신한 총 수신자 수
received_conn_auth_success	SMTP AUTH 명령으로 인증하여 성공한 총 수신 연결 수
received_conn_total	총 수신 연결 수
received_noauth	수신한 총 비인증 수신자 수
received_conn_auth_fail	SMTP AUTH 명령으로 인증하는 데 실패한 총 수신 연결 수
received_conn_noauth	인증 시도 없는 총 수신 연결 수
received_conn_cert_fail	클라이언트 인증서로 인증하는 데 실패한 총 수신 연결 수

mail_dlp_outgoing_traffic_summary

설명

발신 메일에서 발생한 DLP(data loss prevention) 정책 위반 사고 요약

웹 인터페이스의 보고서

Monitor(모니터링) > DLP Incident Summary(DLP 사고 요약) > Top Incidents by Severity(심각도 기준 상위 사고)

카운터	설명
total_dlp_incidents	총 DLP 사고 수
dlp_incidents_high	높음 심각도인 총 DLP 사고 수
dlp_incidents_critical	중대 심각도인 총 DLP 사고 수
dlp_incidents_medium	중간 심각도인 총 DLP 사고 수
dlp_incidents_low	낮음 심각도인 총 DLP 사고 수

mail_incoming_malware_threat_file_detail_summary

설명

수신 메일에서 AMP(Advanced Malware Protection)가 탐지한 악성코드 위협 파일에 대한 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Advanced Malware Protection(지능형 위협 차단) > Top Incoming Malware Threat Files(상위 수신 악성코드 위협 파일)

카운터	설명
detected_amp_files	AMP로 탐지되는 총 악성코드 위협 파일 수

mail_incoming_traffic_summary

설명

어플라이언스에 일어나는 수신 메일 활동의 요약

웹 인터페이스의 보고서

Monitor(모니터링) > Overview(개요) > Incoming Mail Graph(수신 메일 그래프)

카운터	설명
verif_decrypt_success	S/MIME 게이트웨이 확인 및 해독의 일환으로 성공적으로 확인하거나 해독한 총 수신 메시지(수신자) 수
detected_virus	바이러스 양성으로 확인된 메시지(수신자) 수
threat_content_filter	삭제, 반송, 격리 작업의 콘텐츠 필터를 하나 이상 트리거한 메시지(수신자) 수

카운터	설명
verif_decrypt_fail	S/MIME 게이트웨이 확인 및 해독의 일환으로 확인 또는 해독에 실패한 총 수신 메시지(수신자) 수
blocked_dmarc	DMARC에서 차단한 총 메시지(수신자) 수
marketing_mail	마케팅 메일로 탐지된 총 메시지(수신자) 수
detected_amp	AMP에서 악성코드로 탐지한 총 메시지(수신자) 수
ims_spam_increment_over_case	IPAS에서 정상으로 분류했을 가능성이 있으나 IMS에서 스팸으로 분류한 수신 메시지(수신자)
total_recipients	총 메시지(수신자) 수
detected_spam	스팸으로 확인되거나 의심되는 메시지(수신자) 수. 이 값은 구성된 모든 안티스팸 엔진에서 탐지한 스팸 메시지 수를 합한 것입니다.
total_clean_recipients	총 정상 메시지(수신자) 수
blocked_invalid_recipient	수신자 승인 정책에서 거부한 메시지(수신자) 수
malicious_url	악성으로 확인된 URL(수신자) 수
total_threat_recipients	어플라이언스에서 탐지한 총 위협 메시지(수신자) 수
blocked_reputation	평판 필터링에서 차단한 메시지 수

mail_outgoing_traffic_summary

설명

어플라이언스에 일어나는 발신 메일 활동 요약

웹 인터페이스의 보고서

Monitor(모니터링) > Overview(개요) > Outgoing Mail Graph(발신 메일 그래프)

카운터	설명
detected_virus	바이러스 양성으로 확인된 메시지 수
threat_content_filter	삭제, 반송, 격리 작업의 콘텐츠 필터를 하나 이상 트리거한 메시지(수신자) 수
total_dlp_incidents	DLP에서 차단한 총 메시지(수신자) 수
total_clean_recipients	총 정상 메시지(수신자) 수
total_recipients_processed	정상 메시지, 바이러스 메시지, 스팸 메시지 또는 필터에 의해 차단된 메시지(수신자)의 총 개수
total_recipients	총 메시지(수신자) 수
detected_spam	스팸으로 확인되거나 의심되는 메시지(수신자) 수. 이 값은 구성된 모든 안티스팸 엔진에서 탐지한 스팸 메시지 수를 합한 것입니다.
total_hard_bounces	목적지 서버에서 하드 반송한 총 메시지(수신자) 수
malicious_url	악성으로 식별된 URL 수
total_recipients_delivered	전달된 총 메시지(수신자) 수

mail_security_summary

설명

수신 및 발신 메일의 TLS(Transport Layer Security) 요약

웹 인터페이스의 보고서

Monitor(모니터링) > TLS Connections(TLS 연결) > Incoming TLS Connections Graph(수신 TLS 연결 그래프)

카운터	설명
sent_conn_plain	암호화되지 않은 총 발신 연결 수
received_unencrypted	수신 메일의 암호화되지 않은 총 메시지(수신자) 수
received_total	수신한 총 수신자
received_conn_tls_success	성공적인(TLS 필요) 총 수신 TLS 연결 수
received_conn_total	총 수신 연결 수
sent_total	전송한 총 수신자
sent_unencrypted	발신 메일에서 암호화되지 않은 총 메시지(수신자) 수
received_conn_tls_opt_fail	실패한(TLS 기본) 총 수신 TLS 연결 수
sent_conn_tls_opt_success	성공한(TLS 기본) 총 발신 TLS 연결 수
sent_conn_total	총 발신 연결 수
sent_conn_tls_opt_fail	실패한(TLS 기본) 총 발신 TLS 연결 수
received_encrypted_tls	수신 메일의 총 TLS 암호화 메시지(수신자) 수
sent_conn_tls_fail	실패한(TLS 필수) 총 발신 TLS 연결 수
received_conn_tls_opt_success	성공한(TLS 기본) 총 수신 TLS 연결 수
received_conn_plain	암호화되지 않은 총 수신 연결 수
sent_conn_tls_success	성공한(TLS 필수) 총 발신 TLS 연결 수
sent_encrypted_tls	발신 메일의 총 TLS 암호화 메시지(수신자) 수
received_conn_tls_fail	실패한(TLS 필수) 총 수신 TLS 연결 수

mail_sender_group_summary

설명

어플라이언스의 모든 발신자 그룹에 대한 메일 플로우 정책 작업에 의한 연결의 요약

웹 인터페이스의 보고서

Monitor(모니터링) > TLS Connections(TLS 연결) > Incoming TLS Connections Graph(수신 TLS 연결 그래프)

카운터	설명
connections_relay	릴레이 메일 플로우 정책 작업이 수행된 총 연결 수
connections_reject	거부 메일 플로우 정책 작업이 수행된 총 연결 수

카운터	설명
connections_accept	수락 메일 플로우 정책 작업이 수행된 총 연결 수
connections_tcp_refuse	TCP 거절 메일 플로우 정책 작업이 수행된 총 연결 수

mail_system_capacity

설명

어플라이언스의 시스템 용량 매개변수 요약

웹 인터페이스의 보고서

Monitor(모니터링) > System Capacity(시스템 용량) > Work Queue(작업 큐)

카운터	설명
workqueue_average_time_spent	작업 큐에서 소요된 평균 시간(분)
overall_percent_cpu_usage_for_reporting	보고를 위한 전체 평균 CPU 사용률
outgoing_connections	총 발신 연결
overall_percent_cpu_usage	전체 평균 CPU 사용률
bytes_in	총 수신 메시지 크기(바이트)
overall_percent_cpu_usage_for_antivirus	안티바이러스의 전체 평균 CPU 사용률
overall_percent_cpu_usage_for_quarantine	격리의 전체 평균 CPU 사용률
average_incoming_message_size_in_bytes	평균 수신 메시지 크기(바이트)
overall_percent_cpu_usage_for_antispam	안티스팸의 전체 평균 CPU 사용률
average_outgoing_message_size_in_bytes	평균 발신 메시지 크기(바이트)
overall_percent_cpu_usage_for_mail_count	메일 처리의 전체 평균 CPU 사용률
workqueue_average_messages	작업 큐의 평균 메시지
bytes_out	총 발신 메시지 크기(바이트)
outgoing_messages	총 발신 메시지
average_memory_page_swapping	평균 메모리 페이지 스와핑
incoming_connections	총 수신 연결
incoming_messages	총 수신 메시지
workqueue_messages_max	작업 큐의 최대 메시지

상위 N 보고서

- mail_authentication_incoming_domain_ip
- mail_content_filter_incoming
- mail_dmarc_incoming_traffic_summary
- mail_env_sender_rate_limit
- mail_env_sender_stats
- mail_hvm_msg_filter_stats

- mail_incoming_malware_threat_file_detail
- mail_msg_filter_stats
- mail_sender_group_detail
- mail_subject_stats
- mail_url_category_summary
- mail_url_domain_summary
- mail_url_reputation_summary
- mail_vof_threat_summary
- mail_vof_threats_by_level
- mail_vof_threats_by_threat_type
- mail_vof_threats_by_time_threshold
- mail_vof_threats_by_type
- mail_vof_threats_rewritten_url

mail_authentication_incoming_domain_ip

설명

도메인 IP 주소 기준 수신 이메일 인증에 대한 정보

웹 인터페이스의 보고서

보고서 없음

카운터	설명
last_cert_fallback	수신된 연결에서 도메인 IP 주소로부터 클라이언트 인증이 SMTP AUTH 명령으로 대체된 마지막 시점
last_cert_success	성공적으로 수신된 연결에서 도메인 IP 주소로부터 클라이언트 인증서를 사용하여 인증한 마지막 시점
last_auth_disallow	수신된 연결에서 도메인 IP 주소로부터 SMTP AUTH 명령을 사용한 인증이 거부된 마지막 시점
last_cert_fail	수신된 연결에서 도메인 IP 주소로부터 클라이언트 인증서를 사용한 인증에 실패한 마지막 시점
last_auth_success	성공적으로 수신된 연결에서 도메인 IP 주소로부터 SMTP AUTH 명령을 사용하여 인증한 마지막 시점
last_auth_fail	수신된 연결에서 도메인 IP 주소로부터 SMTP AUTH 명령을 사용하는 인증에 실패한 마지막 시점

mail_content_filter_incoming

설명

수신 콘텐츠 필터 매치의 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Content Filters(콘텐츠 필터) > Top Incoming Content Filter Matches(상위 수신 콘텐츠 필터 매치)

카운터	설명
recipients_matched	콘텐츠 필터와 매치하는 총 수신 수신자 수

mail_dmarc_incoming_traffic_summary

설명

수신 메일에 대한 DMARC 검증 정보

웹 인터페이스의 보고서

Monitor(모니터링) > DMARC Verification Report(DMARC 검증 보고서) > Top Domains by DMARC Verification Failures(DMARC 검증 실패 기준 상위 도메인)

카운터	설명
dmarc_total_attempted	도메인 기준으로 DMARC 검증 대상인 총 메시지(수신자) 수
dmarc_failed_total	도메인 기준으로 DMARC 검증을 통과하지 못한 총 메시지(수신자) 수
dmarc_failed_rejected	도메인 기준으로 DMARC 검증을 통과하지 못했고 거부된 총 메시지(수신자) 수
dmarc_failed_none	도메인 기준으로 DMARC 검증을 통과하지 못했고 어떤 조치도 없었던 총 메시지(수신자) 수
dmarc_failed_quarantined	도메인 기준으로 DMARC 검증을 통과하지 못했고 격리된 총 메시지(수신자) 수
dmarc_passed	도메인 기준으로 DMARC 검증을 통과한 총 메시지(수신자) 수

mail_env_sender_rate_limit

설명

속도 제한 정책 위반자 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Rate Limits(속도 제한) > Top Offenders by Incident(사고 기준 상위 위반자)

카운터	설명
env_sender_incidents	envelope 발신자 기준 총 사고 수
env_sender_rejected_rcpts	거절된 발신자 기준 총 사고 수

mail_env_sender_stats

설명

envelope 발신자 기준 메시지 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > High Volume Mail(대용량 메일) > Top Envelope Senders(상위 Envelope 발신자)

카운터	설명
num_msgs	envelope 발신자가 보낸 총 메시지 수

mail_hvm_msg_filter_stats

설명

HVM(High Volume Mail) 메시지 필터(Header Repeats 규칙 사용) 통계

웹 인터페이스의 보고서

Monitor(모니터링) > High Volume Mail(대용량 메일) > Top Message Filters by Number of Matches(매치 수 기준 상위 메시지 필터)

카운터	설명
num_matches	필터와 매치하는 총 메시지 수

mail_incoming_malware_threat_file_detail

설명

수신 메일에서 AMP(Advanced Malware Protection)가 탐지한 악성코드 위협 파일에 대한 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Advanced Malware Protection(지능형 위협 차단) > Top Incoming Malware Threat Files(상위 수신 악성코드 위협 파일)

카운터	설명
detected_amp_files	AMP로 탐지되는 총 악성코드 위협 파일 수

mail_msg_filter_stats

설명

어플라이언스의 메시지 필터 매치 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링)> Message Filters(메시지 필터) > Top Message Filters by Number of Matches(매치 수 기준 상위 메시지 필터)

카운터	설명
num_matches	메시지 필터와 매치하는 총 메시지(수신자) 수

mail_sender_group_detail

설명

발신자 그룹 기준 연결 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Sender Groups> Connections by Sender Group(발신자 그룹 기준 연결)

카운터	설명
total_connections	발신자 그룹 기준 총 연결 수

mail_subject_stats

설명

어플라이언스에서 수신한 메시지 제목의 통계

웹 인터페이스의 보고서

Monitor(모니터링) > High Volume Mail(대용량 메일) > Top Subjects(상위 제목)

카운터	설명
num_msgs	제목 기준 총 메시지(수신자) 수

mail_url_category_summary

설명

수신 및 발신 메일에 나타나는 URL 범주 정보

웹 인터페이스의 보고서

Monitor(모니터링) > URL Filtering(URL 필터링) > Top URL Categories in Incoming Messages(수신 메시지의 상위 URL 범주)

카운터	설명
outgoing_count	발신 메시지의 URl 범주 분포
incoming_count	수신 메시지의 URl 범주 분포

mail_url_domain_summary

설명

수신 및 발신 스팸 메시지에 나타나는 URL 도메인 정보

웹 인터페이스의 보고서

Monitor(모니터링) > URL Filtering(URL 필터링) > Top URLs in Incoming Spam Messages(수신 스팸 메시지의 상위 URL)

카운터	설명
outgoing_count	발신 스팸 메시지의 도메인 기준 URL 수
incoming_count	수신 스팸 메시지의 도메인 기준 URL 수

mail_url_reputation_summary

설명

수신 및 발신 메시지에 나타나는 악성 URL 및 의심스러운 URL에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > URL Filtering(URL 필터링) > Summary of Incoming Messages Containing Malicious and Suspicious URLs(악성 URL 및 의심스러운 URL을 포함하는 수신 메시지 요약)

카운터	설명
outgoing_count	발신 메시지의 URL 평판 분포
incoming_count	수신 메시지의 URL 평판 분포

mail_vof_threat_summary

설명

신종 바이러스 필터에서 탐지한 위협에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터) > Threat Summary(위협 요약)

카운터	설명
threat_detected	위협 범주 기준으로 신종 바이러스 필터에서 탐지한 위협 수

mail_vof_threats_by_level

설명

신종 바이러스 필터에서 탐지한 위협의 심각도에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터) > Hit Messages by Threat Level(위협 레벨 기준 해당 메시지)

카운터	설명
threat_detected	위협 레벨 기준으로 신종 바이러스 필터에서 탐지한 위협 수

mail_vof_threats_by_threat_type

설명

신종 바이러스 필터에서 탐지한 위협 유형에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터) > Hit Messages from Incoming Messages(수신 메시지의 해당 메시지)

카운터	설명
threat_detected	위협 유형 기준으로 신종 바이러스 필터에서 탐지한 위협 수

mail_vof_threats_by_time_threshold

설명

OF(Outbreak Filter) 쿼런틴의 메시지에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터) > Messages resided in Outbreak Quarantine(신종 바이러스 쿼런틴에 있는 메시지)

카운터	설명
quarantine_message_exit	쿼런틴에서 보낸 시간 기준 신종 바이러스 필터가 격리한 메시지 수

mail_vof_threats_by_type

설명

신종 바이러스 필터에서 탐지한 위협 유형에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터) > Threats by Type(유형 기준 위협)

카운터	설명
threat_detected	위협 유형 기준으로 신종 바이러스 필터에서 탐지한 위협 수

mail_vof_threats_rewritten_url

설명

신종 바이러스 필터에 의해 다시 쓰여진 URL 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터) > Top URL's Rewritten(다시 쓰여진 상위 URL)

카운터	설명
rewritten_url	URL 기준으로 신종 바이러스 필터에 의해 다시 쓰여진 URL 수

쿼리 관련 보고서

- mail_authentication_incoming_domain
- mail_content_filter_outgoing
- mail_destination_domain_detail
- mail_dlp_outgoing_policy_detail
- mail_incoming_domain_detail
- mail_incoming_ip_hostname_detail
- mail_incoming_network_detail
- mail_sender_domain_detail
- mail_sender_ip_hostname_detail
- mail_users_detail
- mail_virus_type_detail

mail_authentication_incoming_domain

설명

도메인 기준으로 수신 메일에서 발생하는 SMTP 인증 통계의 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Inbound SMTP Authentication(인바운드 SMTP 인증) > SMTP Authentication Details By Domain Name(도메인 이름 기준 SMTP 인증 세부 정보)

엔티티 값

도메인 이름

카운터	설명
cert_fallback_success	도메인의 클라이언트 인증서에서 SMTP AUTH 명령으로 대체하여 인증한 총 수신 연결 수
cert_fallback_fail	도메인의 클라이언트 인증서에서 SMTP AUTH 명령으로 대체하여 인증하는 데 실패한 총 수신 연결 수
auth_disallow	도메인에서 SMTP AUTH 명령을 사용한 인증이 거부된 총 수신 연결 수
auth_fail	도메인에서 SMTP AUTH 명령을 사용한 인증에 실패한 총 수신 연결 수
cert_success	도메인에서 클라이언트 인증서를 사용하여 인증한 총 수신 연결 수
noauth	인증 시도 없는 총 수신 연결 수
auth_success	도메인에서 SMTP AUTH 명령을 사용하여 인증한 총 수신 연결 수
cert_fail	도메인에서 클라이언트 인증서를 사용한 인증에 실패한 총 수신 연결 수
total	총 수신 연결 수

mail_content_filter_outgoing

설명
발신 콘텐츠 필터 매치 세부 정보

웹 인터페이스의 보고서
보고서 없음

엔티티 값
발신 콘텐츠 필터의 이름

카운터	설명
recipients_matched	콘텐츠 필터와 매치하는 총 발신 수신자 수

mail_destination_domain_detail

설명
목적지 도메인에 보낸 메시지 세부 정보

웹 인터페이스의 보고서
Monitor(모니터링) > Outgoing Destinations(발신 목적지) > Top Destinations by Total Threat Messages(총 위협 메시지 기준 상위 목적지)

엔티티 값
도메인 이름

카운터	설명
제공:	목적지 도메인에 전달한 총 메시지(수신자)
detected_virus	목적지 도메인에 보냈고 바이러스 양성으로 확인된 메시지(수신자) 수
encrypted_tls	TLS를 사용하여 보낸 총 메시지(수신자) 수
threat_content_filter	목적지 도메인에 보냈고 삭제, 반송, 격리 작업의 콘텐츠 필터를 하나 이상 트리거한 메시지(수신자) 수
conn_tls_total	TLS를 사용하여 보낸 총 연결 수
conn_tls_opt_fail	목적지 도메인 기준으로 실패한(TLS 기본) 총 TLS 연결 수
total_clean_recipients	목적지 도메인에 보낸 정상 메시지(수신자) 수
total_recipients_processed	목적지 도메인에 보낸 정상 메시지, 바이러스 메시지, 스팸 메시지 또는 필터에 의해 차단된 메시지(수신자)의 총 개수
conn_tls_opt_success	목적지 도메인 기준으로 성공한(TLS 기본) 총 TLS 연결 수
conn_plain	총 비 TLS 연결 수
conn_tls_success	목적지 도메인 기준으로 성공한(TLS 필수) 총 TLS 연결 수
total_recipients	목적지 도메인에 보낸 총 메시지(수신자)
conn_tls_fail	목적지 도메인 기준으로 실패한(TLS 필수) 총 TLS 연결 수
detected_spam	목적지 도메인에 보냈고 스팸으로 확인되었거나 의심되는 메시지(수신자) 수
conn_last_tls_status	마지막 TLS 연결 상태
hard_bounces	목적지 도메인에 보냈고 목적지 서버에서 하드 반송한 총 메시지(수신자) 수
total_threat_recipients	목적지 도메인에 보낸 총 위협 메시지(수신자) 수

mail_dlp_outgoing_policy_detail

설명

발신 메일에서 발생한 DLP(data loss prevention) 정책 위반 사고 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > DLP Incident Summary(DLP 사고 요약) > Top DLP Policy Matches(상위 DLP 정책 매치)

엔티티 값

DLP 정책 이름

카운터	설명
dlp_action_dropped	포기한 DLP 정책과 매치하는 총 수신자(메시지) 수
dlp_incidents_high	정책 매치 기준으로 높음 심각도인 총 DLP 사고 수
dlp_incidents_critical	정책 매치 기준으로 중대 심각도인 총 DLP 사고 수
dlp_action_encrypted	전달한 (암호화된) DLP 정책과 매치하는 총 수신자(메시지) 수

카운터	설명
total_dlp_incidents	총 DLP 사고 수
dlp_action_delivered	전달한 (암호화되지 않은) DLP 정책과 매치하는 총 수신자(메시지) 수
dlp_incidents_medium	정책 매치 기준으로 중간 심각도인 총 DLP 사고 수
dlp_incidents_low	정책 매치 기준으로 낮음 심각도인 총 DLP 사고 수

mail_incoming_domain_detail

설명

연결하는 도메인에 대한 수신 메일 활동의 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Incoming Mail Domains(수신 메일 도메인) > Top DLP Policy Matches(상위 DLP 정책 매치)

엔티티 값

도메인 이름

카운터	설명
total_throttled_recipients	도메인 기준으로 조절된 총 수신자 수
conn_tls_total	도메인 기준 총 TLS 연결 수
detected_virus	도메인 기준으로 바이러스 양성으로 확인된 총 메시지(수신자) 수
total_rejected_connections	도메인 기준으로 거부된 총 연결 수
total_accepted_connections	도메인 기준으로 수락된 총 연결 수
threat_content_filter	도메인 기준으로 콘텐츠 필터에 의해 차단된 총 메시지(수신자) 수
conn_tls_opt_fail	도메인 기준으로 실패한(TLS 기본) 총 TLS 연결 수
blocked_invalid_recipient	도메인 기준으로 유효하지 않은 총 수신자 수
blocked_dmarc	도메인 기준으로 DMARC 검증 때문에 차단된 총 메시지(수신자) 수
marketing_mail	도메인 기준으로 마케팅 메일로 확인된 총 메시지(수신자) 수
conn_plain	도메인 기준 총 비 TLS 연결 수
detected_amp	도메인 기준으로 AMP에서 확인한 총 메시지(수신자) 수
conn_tls_success	도메인 기준으로 성공한(TLS 필수) 총 TLS 연결 수
total_recipients	도메인 기준으로 시도한 총 수신자 수
conn_tls_fail	도메인 기준으로 실패한(TLS 필수) 총 TLS 연결 수
detected_spam	도메인 기준으로 스팸으로 확인되었거나 의심되는 총 메시지(수신자) 수
encrypted_tls	TLS를 통해 전송되는 총 메시지(수신자) 수
total_clean_recipients	도메인 기준 총 정상 메시지(수신자) 수
total_threat_recipients	도메인 기준 총 위협 메시지(수신자) 수
blocked_reputation	도메인 기준으로 평판 필터링된 총 수신자 수
conn_tls_opt_success	도메인 기준으로 성공한(TLS 기본) 총 TLS 연결 수

mail_incoming_ip_hostname_detail

설명

IP 주소와 호스트 이름을 연결하는 수신 메일 활동에 대한 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Incoming Mail IP Addresses(수신 메일 IP 주소) > Top Senders by Total Threat Messages(총 위협 메시지 기준 상위 발신자)

엔티티 값

IPv4 또는 IPv6 주소

카운터	설명
dns_verified	IP에 대해 검증된 DNS
detected_virus	IP 기준으로 바이러스 양성으로 확인된 총 메시지(수신자) 수
threat_content_filter	IP 기준으로 삭제, 반송, 격리 작업의 콘텐츠 필터를 하나 이상 트리거한 총 메시지(수신자) 수
blocked_invalid_recipient	IP 기준으로 유효하지 않은 총 수신자 수
blocked_dmarc	IP 기준으로 DMARC 검증 실패 때문에 차단된 총 메시지(수신자) 수
marketing_mail	IP 기준으로 마케팅 메일로 탐지된 총 메시지(수신자) 수
detected_amp	IP 기준으로 AMP 양성으로 확인된 총 메시지(수신자) 수
last_sender_group_name	IP에 대한 발신자 그룹 이름
sbrs_score	IP에 대한 SBRS 점수
total_recipients	IP 기준으로 시도된 총 수신자 수
detected_spam	IP 기준으로 스팸으로 확인되었거나 의심되는 총 메시지(수신자) 수
total_clean_recipients	IP 기준으로 총 정상 메시지(수신자) 수
total_threat_recipients	IP 기준으로 총 스팸, 바이러스, 위협 필터 메시지(수신자) 수
blocked_reputation	IP 기준으로 평판 필터링된 총 수신자 수

mail_incoming_network_detail

설명

네트워크 소유자에 대한 수신 메일 활동의 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Incoming Mail Network Owners(수신 메일 네트워크 소유자) > Top Senders by Total Threat Messages(총 위협 메시지 기준 상위 발신자)

엔티티 값

네트워크 소유자의 이름

카운터	설명
total_throttled_recipients	네트워크 소유자에 대해 조절된 총 연결 수
detected_virus	네트워크 소유자에 대해 바이러스 양성으로 확인된 총 메시지(수신자) 수
total_threat_recipients	네트워크 소유자에 대한 총 위협 수신자 수
total_accepted_connections	네트워크 소유자에 대해 수락된 총 연결 수
threat_content_filter	네트워크 소유자에 대해 삭제, 반송, 격리 작업의 콘텐츠 필터를 하나 이상 트리거한 총 메시지(수신자) 수
blocked_invalid_recipient	네트워크 소유자에 대해 유효하지 않은 총 수신자 수
blocked_dmarc	네트워크 소유자에 대해 DMARC 검증 실패 때문에 차단된 총 메시지(수신자) 수
marketing_mail	네트워크 소유자에 대해 마케팅 메일로 탐지된 총 메시지(수신자) 수
detected_amp	네트워크 소유자에 대해 AMP 양성으로 확인된 총 메시지(수신자) 수
total_recipients	네트워크 소유자에 대한 총 수신자 수
detected_spam	네트워크 소유자에 대해 스팸으로 확인되었거나 의심되는 총 메시지(수신자) 수
total_clean_recipients	네트워크 소유자에 대한 총 정상 메시지(수신자) 수
total_rejected_connections	네트워크 소유자에 대해 거부된 총 연결 수
blocked_reputation	네트워크 소유자에 대해 위협 필터링된 총 수신자 수

mail_sender_domain_detail

설명

발신 콘텐츠 필터 매치 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Outgoing Senders Domains(발신자 도메인) > Top Senders by Total Threat Messages(총 위협 메시지 기준 상위 발신자)

엔티티 값

도메인 이름

카운터	설명
detected_virus	도메인에서 바이러스 양성으로 확인된 총 메시지(수신자) 수
threat_content_filter	도메인에서 콘텐츠 필터에 의해 차단된 총 메시지(수신자) 수
total_dlp_incidents	도메인에서 총 DLP 사고 수
total_clean_recipients	도메인에서 총 정상 메시지(수신자) 수
total_recipients_processed	도메인에서 정상 메시지, 바이러스 메시지, 스팸 메시지 또는 필터에 의해 차단된 메시지의 총 개수

카운터	설명
detected_spam	도메인에서 스팸으로 확인되었거나 의심되는 총 메시지(수신자) 수
total_threat_recipients	도메인에서 총 위협 수신자 수

mail_sender_ip_hostname_detail

설명

메시지를 보내는 내부 IP 및 호스트 이름의 세부 정보.

웹 인터페이스의 보고서

Monitor(모니터링) > Outgoing Senders IP Addresses(발신자 IP 주소) > Top Senders by Total Threat Messages(총 위협 메시지 기준 상위 발신자)

엔티티 값

IPv4 또는 IPv6 주소

카운터	설명
detected_virus	IP에서 바이러스 양성으로 확인된 총 메시지(수신자) 수
threat_content_filter	IP에서 콘텐츠 필터에 의해 차단된 총 메시지(수신자) 수
total_dlp_incidents	IP에서 총 DLP 사고 수
total_clean_recipients	IP에서 발신 메일의 총 정상 메시지(수신자) 수
total_recipients_processed	IP에서 안전하거나 위협으로 확인된 총 메시지(수신자) 수
detected_spam	IP에서 스팸으로 확인되었거나 의심되는 총 메시지(수신자) 수
total_threat_recipients	IP에서 총 위협 수신자 수

mail_users_detail

설명

어플라이언스를 통해 내부 사용자(이메일 주소 기준)가 보내고 받은 메일에 대한 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Internal Users(내부 사용자) > Top Users by Clean Incoming Messages(정상 수신 메시지 기준 상위 사용자)

엔티티 값

내부 사용자의 이메일 주소

카운터	설명
incoming_detected_amp	AMP 양성으로 확인된 수신 메시지(수신자)
outgoing_detected_content_filter	콘텐츠 필터와 매치하는 발신 메시지(수신자)
incoming_marketing_mail	수신 마케팅 메시지(수신자)

카운터	설명
outgoing_detected_spam	스팸으로 확인되거나 의심되는 발신 메시지(수신자) 수 이 값은 구성된 모든 안티스팸 엔진에서 탐지한 스팸 메시지 수를 합한 것입니다.
incoming_threat_content_filter	콘텐츠 필터에 의해 차단된 수신 메시지(수신자)
incoming_total_clean_recipients	총 수신 정상 메시지(수신자)
incoming_detected_spam	스팸으로 확인되거나 의심되는 수신 메시지(수신자) 수 이 값은 구성된 모든 안티스팸 엔진에서 탐지한 스팸 메시지 수를 합한 것입니다.
incoming_detected_content_filter	콘텐츠 필터와 매치하는 수신 메시지(수신자)
incoming_detected_virus	바이러스 양성으로 확인된 수신 메시지(수신자)
outgoing_detected_virus	바이러스 양성으로 확인된 발신 메시지(수신자)
incoming_detected_ims_spam_increment_over_case	IPAS에서 정상으로 분류했을 가능성이 있으나 IMS에서 스팸으로 분류한 수신 메시지(수신자)
outgoing_total_clean_recipients	총 발신 정상 메시지(수신자)
outgoing_threat_content_filter	콘텐츠 필터에 의해 차단된 발신 메시지(수신자)
outgoing_detected_ims_spam_increment_over_case	IPAS에서 정상으로 분류했을 가능성이 있으나 IMS에서 스팸으로 분류한 발신 메시지(수신자)

mail_virus_type_detail

설명

어플라이언스에서 식별된 상위 수신 및 발신 바이러스 유형의 세부 정보

웹 인터페이스의 보고서

Monitor(모니터링) > Virus Types(바이러스 유형) > Top Incoming Virus Types Detected(탐지된 상위 수신 바이러스 유형)

엔티티 값

바이러스 이름

카운터	설명
total_recipients	상위 n개 바이러스 유형에 감염된 총 수신 및 발신 메시지(수신자) 수. 여기서 n은 사용자가 지정한 값입니다. 기본값은 상위 10개입니다.
incoming_total_recipients	상위 n개 바이러스 유형에 감염된 총 수신 메시지(수신자) 수. 여기서 n은 사용자가 지정한 값입니다. 기본값은 상위 10개입니다.
outgoing_total_recipients	상위 n개 바이러스 유형에 감염된 총 발신 메시지(수신자) 수. 여기서 n은 사용자가 지정한 값입니다. 기본값은 상위 10개입니다.