보안 엔드포인트 프라이빗 클라우드를 보안 웹 및 이메일과 통합

목차

소개

이 문서에서는 Secure Endpoint 프라이빗 클라우드를 SWA(Secure Web Appliance) 및 ESA(Secure Email Gateway)와 통합하는 데 필요한 단계를 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

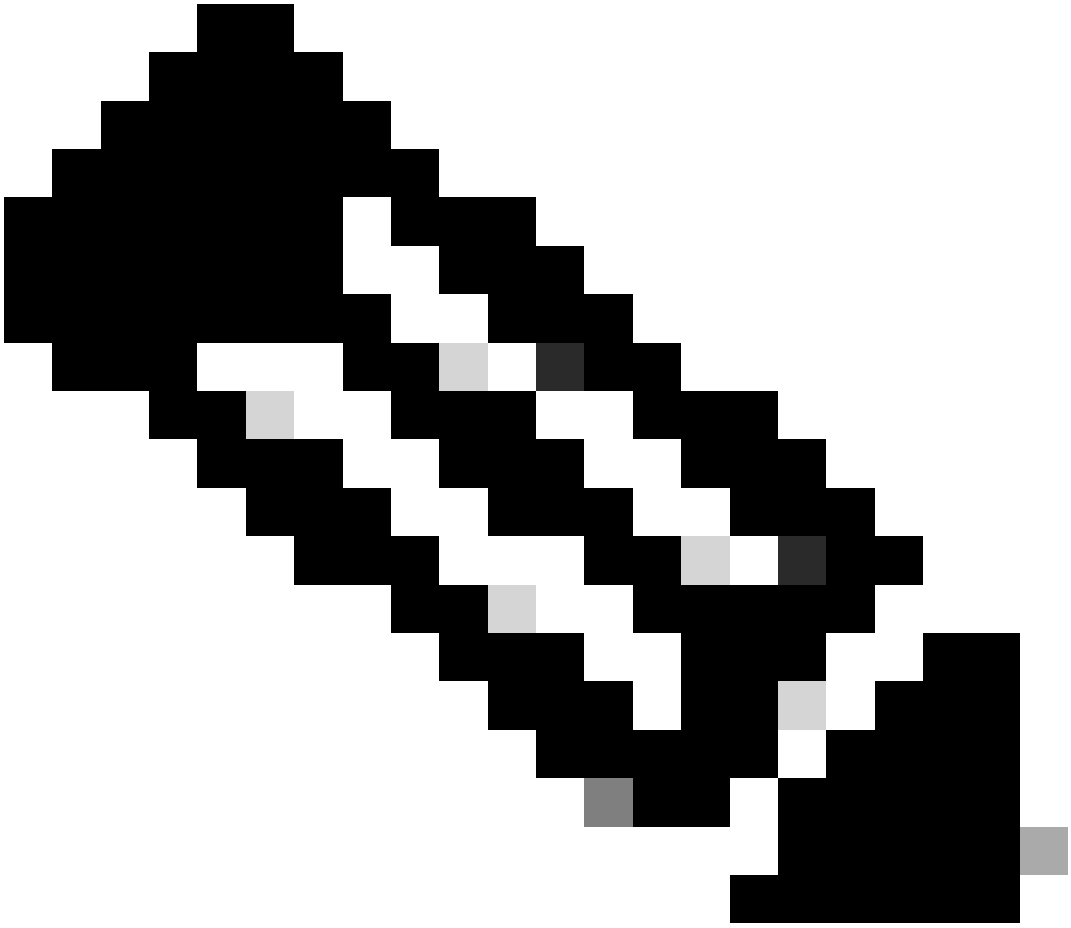
- 보안 엔드포인트 AMP 가상 프라이빗 클라우드
- SWA(Secure Web Appliance)
- 보안 이메일 게이트웨이

사용되는 구성 요소

SWA(Secure Web Appliance) 15.0.0-322

AMP virtual private cloud 4.1.0_202311092226

Secure Email Gateway 14.2.0-620



참고: 이 설명서는 모든 관련 제품의 물리적 및 가상 변형 모두에 유효합니다.

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.

통합을 진행하기 전에 확인

1. 에 필요한 라이센스 **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** 가 있는지 확인합니다. 기능 키를 확인하거나 스마트 **SWA/Secure Email** 라이센스가 활성화되었는지 확인할 수 있습니다.
2. HTTPS 트래픽을 검사하려면 SWA에서 HTTPS 프록시를 활성화해야 합니다. 파일 평판 검사를 수행하려면 HTTPS 트래픽을 해독해야 합니다.
3. AMP Private Cloud/Virtual Private Cloud 어플라이언스 및 필요한 모든 인증서를 구성해야 합니다. 확인은 VPC 인증서 가이드를 참조하십시오.

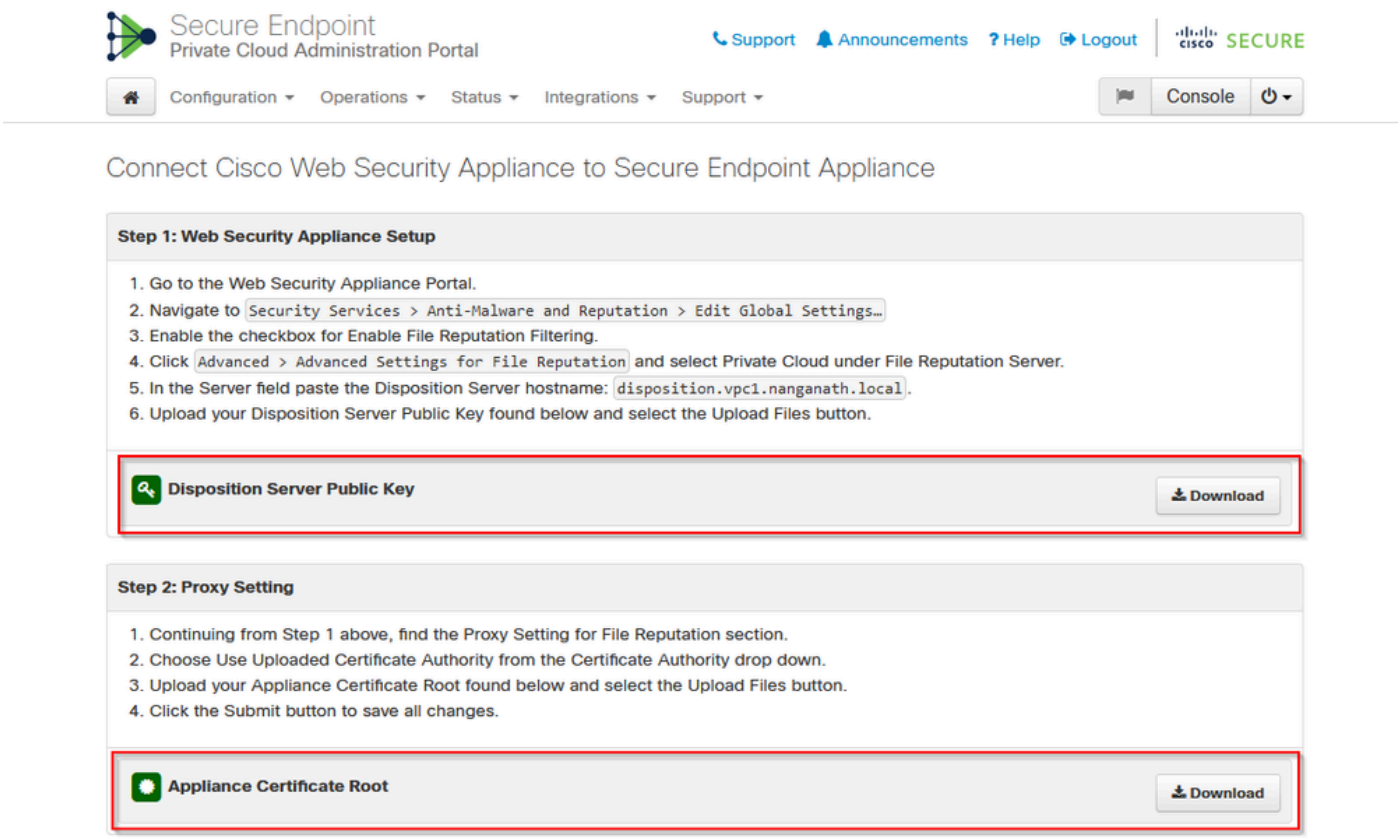
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html

4. 제품의 모든 호스트 이름은 DNS를 확인할 수 있어야 합니다. 이는 통합하는 동안 연결 문제 또는 인증서 문제를 방지하기 위한 것입니다. Secure Endpoint 프라이빗 클라우드에서 Eth0 인터페이스는 관리자 액세스를 위한 것이며 Eth1은 통합 디바이스와 연결할 수 있어야 합니다.

절차

보안 엔드포인트 프라이빗 클라우드 구성

1. 에 **Secure Endpoint VPC admin portal**로그인합니다.
2. **> "Configuration" > "Services" > "Disposition Server"** Copy the disposition server hostname(속성 서버 호스트 이름 복사)으로 이동합니다(세 번째 단계에서도 가져올 수 있음).
3. 로 이동합니다.**"Integrations" > "Web Security Appliance"**
4. 를 **"Disposition Server Public Key" & "Appliance Certificate Root"** 다운로드합니다.
5. 로 이동합니다.**"Integrations" > "Email Security Appliance"**
6. ESA 버전을 선택하고 "Disposition Server Public Key(처리 서버 공개 키)" 및 "Appliance Certificate Root(어플라이언스 인증서 루트)"를 다운로드합니다.
7. 인증서와 키를 모두 안전하게 보관하십시오. 나중에 SWA/보안 이메일에 업로드해야 합니다.

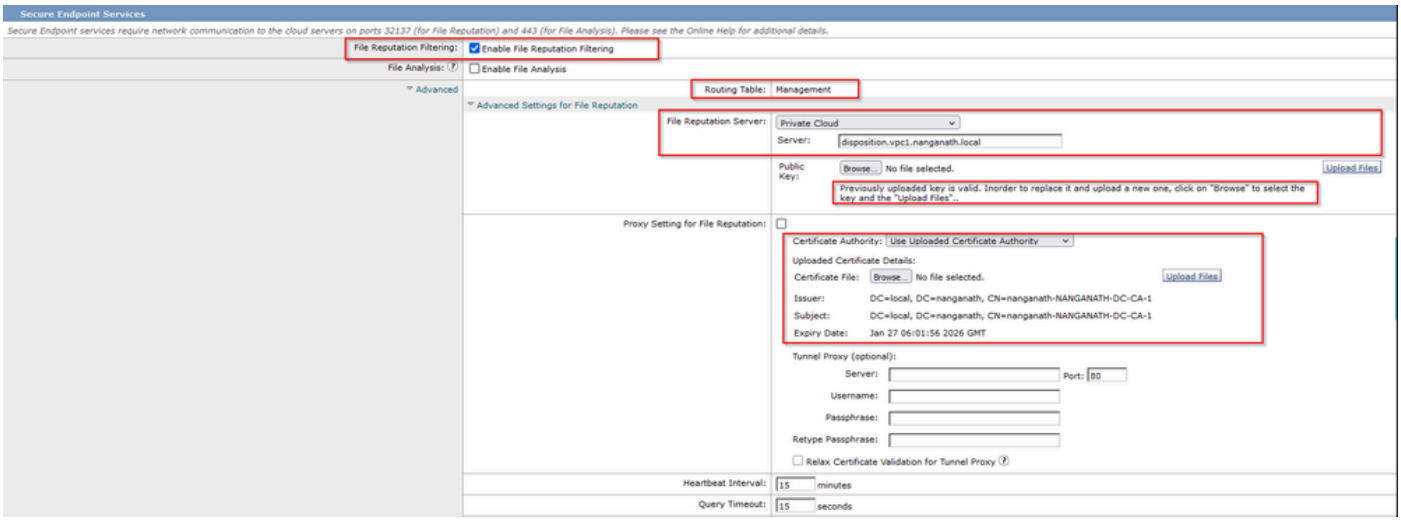


Secure Web Appliance 구성

1. 로 이동합니다 **SWA GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings**
2. "Secure Endpoint Services(보안 엔드포인트 서비스)" 섹션에서 "Enable File Reputation Filtering(파일 평판 필터링 활성화)" 옵션을 볼 수 있으며, "Check(확인)" 이 옵션은 새 필드

"Advanced(고급)"를 표시합니다.

3. File Reputation Server(파일 평판 서버)에서 "Private Cloud(프라이빗 클라우드)"를 선택합니다.
4. 프라이빗 클라우드 Disposition Server 호스트 이름을 "Server"로 제공합니다.
5. 이전에 다운로드한 공개 키를 업로드합니다. "Upload Files(파일 업로드)"를 클릭합니다.
6. 인증 기관을 업로드하는 옵션이 있습니다. 드롭다운에서 "Use Uploaded Certificate Authority(업로드된 인증 기관 사용)"를 선택하고 이전에 다운로드한 CA 인증서를 업로드합니다.
7. 변경 내용 전송
8. 변경 사항 커밋



Cisco Secure Email 구성

1. 다음으로 이동 **Secure Email GUI > Security Services" > "File Reputation and Analysis" > Edit Global Settings > "Enable" or "Edit Global Settings"**

2. File Reputation Server(파일 평판 서버)에서 "Private Cloud(프라이빗 클라우드)"를 선택합니다

3. 프라이빗 클라우드 Disposition Server 호스트 이름을 "Server"로 제공합니다.

4. 이전에 다운로드한 공개 키를 업로드합니다. "Upload Files(파일 업로드)"를 클릭합니다.

5. 인증 기관을 업로드합니다. 드롭다운에서 "Use Uploaded Certificate Authority(업로드된 인증 기관 사용)"를 선택하고 이전에 다운로드한 CA 인증서를 업로드합니다.

6. 변경 사항을 전송합니다.

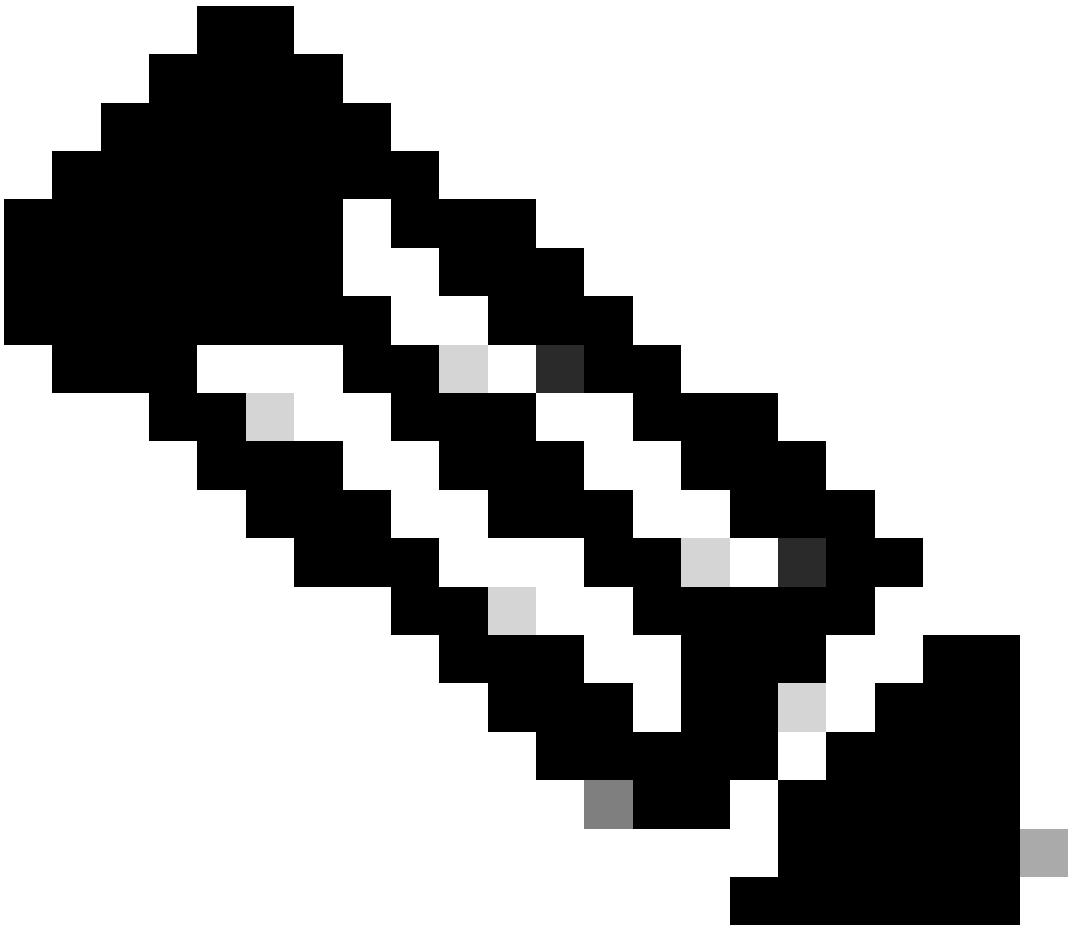
7. 변경 사항을 커밋합니다.

Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 443 (for File Reputation and File Analysis). Please see the Online Help for additional details.

File Reputation Filtering:	☑ Enable File Reputation
File Analysis: ⓘ	☐ Enable File Analysis
▽ Advanced Settings for File Reputation	File Reputation Server: Private reputation cloud Server: disposition.vpc1.nanganath.local Public Key: Browse... No file selected. Upload File *A valid public key has already been uploaded. To upload a new one, click on "Browse" to select the key and then the "Upload File".*
	SSL Communication for File Reputation: Use SSL (Port 443) Tunnel Proxy (Optional): Server: Port: Username: Passphrase: Retype Passphrase: ☐ Relax Certificate Validation for Tunnel Proxy ⓘ
	Heartbeat Interval: 15 minutes
	Query Timeout: 20 seconds
	Processing Timeout: 120 seconds
	File Reputation Client ID: cb1b31fc-9277-4008-a396-6cd486ecc621
	File Retrospective: ☐ Suppress the verdict update alerts ⓘ
▷ Cache Settings	*Advanced settings for Cache*
▷ Threshold Settings	*Advanced Settings for File Analysis Threshold Score*



참고: Cisco Secure Web Appliance 및 Cisco Secure Email Gateway는 AsyncOS를 기반으로 하며 파일 평판이 초기화될 때 거의 동일한 로그를 공유합니다. AMP 로그는 Secure Web Appliance 또는 Secure Email Gateway AMP 로그에서 확인할 수 있습니다(두 디바이스 모두에서 비슷한 로그). 이는 서비스가 SWA 및 Secure Email Gateway에서 초기화되었음을 나타냅니다. 연결이 완전히 성공했음을 나타내지는 않았습니다. 연결 또는 인증서 문제가 있는 경우 "File Reputation initialized(파일 평판 초기화됨)" 메시지 다음에 오류가 표시됩니다. 대부분 "Unreachable error" 또는 "certificate Invalid" 오류를 나타냅니다.

Secure Web 및 Email에서 AMP 로그를 가져오는 단계

1. SWA/Secure Email Gateway CLI에 로그인하고 명령을 입력합니다 **"grep"**

2. 선택 **"amp" or "amp_logs"**

3. 다른 모든 필드를 그대로 두고 "Y"를 입력하여 로그를 미룹니다. 라이브 이벤트를 표시하도록 로그를 미룹니다. 이전 이벤트를 찾는 경우 "정규식"에 날짜를 입력할 수 있습니다.

```
Tue Feb 20 18:17:53 2024 Info:  connecting to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info:  connected to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info:  File reputation service initialized successfully
Tue Feb 20 18:17:53 2024 Info:  The following file type(s) can be sent for File Analysis:Executables, Document,
Microsoft Documents, Database, Miscellaneous, Encoded and Encrypted, Configuration, Email, Archived and compress
ed. To allow analysis of new file type(s), go to Security Services > File Reputation and Analysis.
```

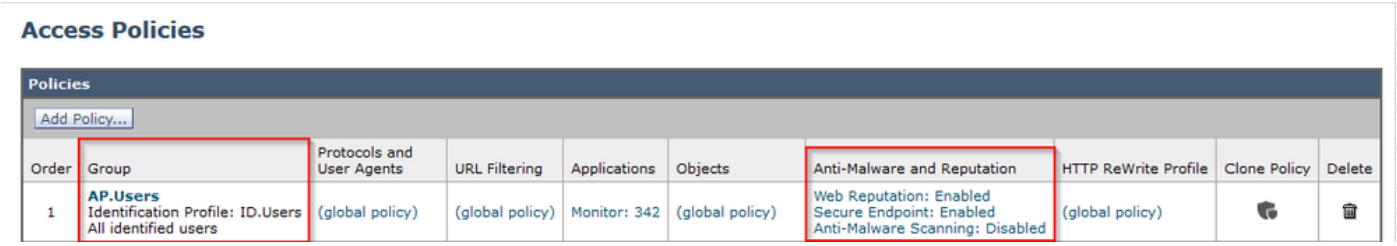
Secure Web Appliance와 Secure Endpoint 프라이빗 클라우드의 통합 테스트

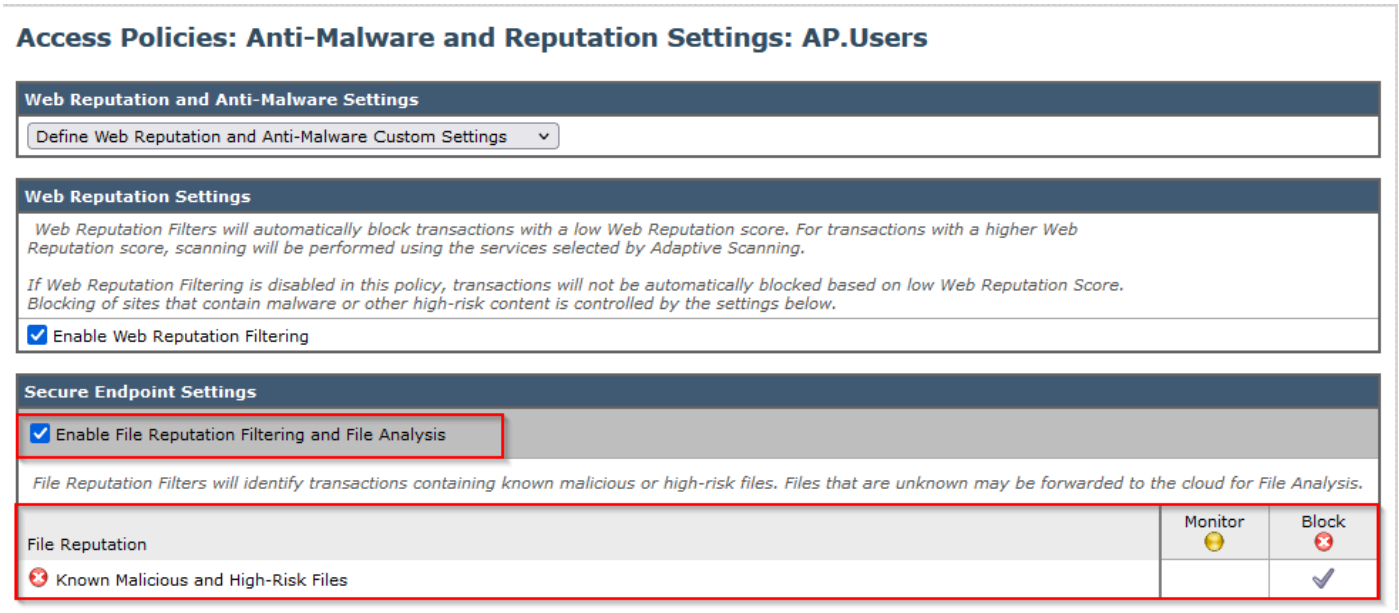
SWA에서 연결을 테스트할 수 있는 직접적인 옵션은 없습니다. 로그 또는 경고를 검사하여 문제가 있는지 확인해야 합니다.

간소화를 위해 HTTPS 대신 HTTP URL을 테스트합니다. 모든 파일 평판 검사를 위해 HTTPS 트래픽을 해독해야 합니다.

컨피그레이션은 SWA 액세스 정책에서 수행되며 AMP 검사를 시행합니다.

참고: Cisco Secure Web Appliance에서 정책을 구성하는 방법을 알아보려면 SWA 사용 설명서를 참조하십시오.





Cisco 보안 웹 어플라이언스를 통해 인터넷에서 악성 파일 "Bombermania.exe.zip"을 다운로드하려고 했습니다. 로그에 악성 파일이 차단된 것으로 표시됩니다.

SWA 액세스 로그

액세스 로그는 다음 단계를 통해 가져올 수 있습니다.

1. SWA에 로그인하고 명령을 입력합니다 "**grep**"

2. 선택 "**accesslogs**"

3. 클라이언트 IP와 같은 "정규식"을 추가하려면 해당 내용을 언급하십시오.

4. "Y"를 입력하여 로그를 미룹니다.

1708320236.640 61255 10.106.37.205 TCP_DENIED/403 2555785 http://static1.1.sqspcdn.com/static/f/830757/21908425/1360688016967/Bombermania.exe.zip?token=gsF - DEFAULT_PARENT/bgl11-lab-wsa-2.cisco.com application/zip BLOCK_AMP_RESP_12-AP.Users-USERS-NONE-NONE-NONE-NONE-DEFAULTGroup-NONE <"IW_comp",3.7,1,"-",-,-,1,"","-","-","IW_comp",-,"AMP High Risk","Computers and Internet" "","알 수 없음","-","-",333.79,0,-,"-","-",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"Bombermania.exe.zip","46ee42fb79a161bf376","-,-,-,-,->

TCP_DENIED/403 —> SWA가 이 HTTP GET 요청을 거부했습니다.

BLOCK_AMP_RESP —> AMP 응답으로 인해 HTTP GET 요청이 차단되었습니다.

Win.Ransomware.Protected::Trojan.Agent.talos —> 위협 이름

Bombermania.exe.zip —> 다운로드하려고 시도한 파일 이름

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 —> 파일의 SHA 값

SWA AMP 로그

다음 단계를 사용하여 AMP 로그를 가져올 수 있습니다.

1. SWA에 로그인하고 명령을 입력합니다 **"grep"**

2. 선택 **"amp_logs"**

3. 다른 모든 필드를 그대로 두고 "Y"를 입력하여 로그를 미룹니다. 라이브 이벤트를 표시하도록 로그를 미룹니다. 이전 이벤트를 찾는 경우 "정규식"에 날짜를 입력할 수 있습니다.

'verdict_from': 'Cloud' 프라이빗 클라우드와 퍼블릭 클라우드의 경우도 마찬가지입니다. 퍼블릭 클라우드의 판정으로 혼동하지 마십시오.

2월 19일 월요일 10:53:56 2024 디버그: 조정된 판정 - {'category': 'amp', 'spyname': 'Win.Ransomware.Protected::Trojan.Agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status': 18, 'verdict_num': 3, 'analysis_score': 0, 'uploaded': False, 'file_name': 'Bombermania.exe.zip', 'verdict_source': None, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud, 'analysis_action': 2, 'application/zip'" , 'upload_reason': '파일 형식이 샌드박싱에 대해 구성되지 않았습니다.', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicious_child': None}

보안 엔드포인트 프라이빗 클라우드 이벤트 로그

이벤트 로그는 **/data/cloud/log**

SHA256을 사용하거나 SWA의 "File Reputation Client ID(파일 평판 클라이언트 ID)"를 사용하여 이벤트를 검색할 수 있습니다. "File Reputation Client ID(파일 평판 클라이언트 ID)"는 SWA의 AMP 컨피그레이션 페이지에 있습니다.

pv - 프로토콜 버전, 3은 TCP

ip - 이 필드가 평판 쿼리를 수행한 클라이언트의 실제 IP 주소를 나타낸다는 보장이 없으므로 이 필드를 무시하십시오.

uu - WSA/ESA의 파일 평판 클라이언트 ID

SHA256 - 파일의 SHA256

dn - 탐지 이름

n - AMP에서 파일 해시를 본 적이 없는 경우 1, 그렇지 않은 경우 0.

rd - 응답 성향. 여기서 3은 DISP_MALICIOUS를 의미합니다.

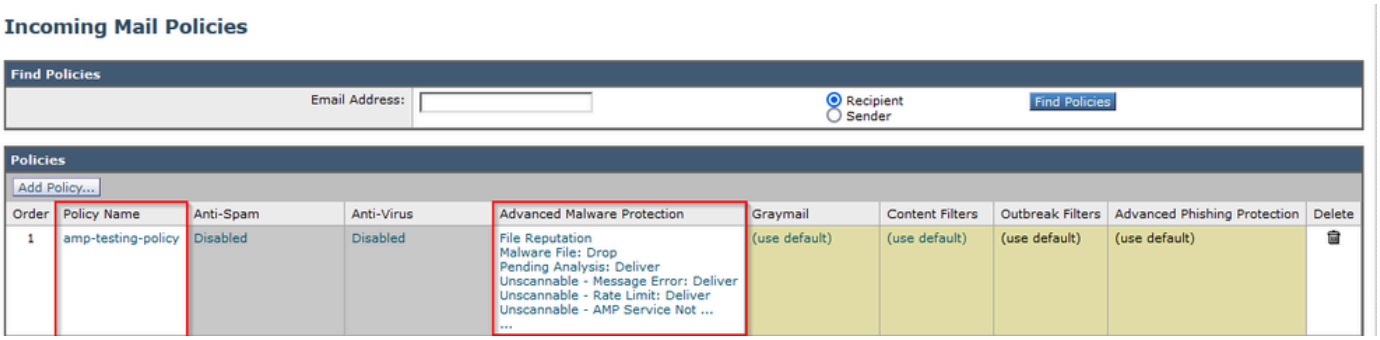
1 DISP_UNKNOWN 파일 속성을 알 수 없습니다.

2 DISP_CLEAN 파일이 정상인 것으로 간주됩니다.
3 DISP_MALICIOUS 파일이 악성으로 간주됩니다.
7 DISP_UNSEEN 파일 속성을 알 수 없으며 파일을 처음 본 것입니다.
13 DISP_BLOCK 파일을 실행하지 않아야 합니다.
14 DISP_IGNORE XXX
15 DISP_CLEAN_PARENT 파일이 안전한 것으로 간주되며 파일이 생성하는 악성 파일은 알 수 없는 것으로 취급해야 합니다.
16 DISP_CLEAN_NFM 파일이 정상으로 간주되지만 클라이언트는 네트워크 트래픽을 모니터링해야 합니다.

Secure Email과 AMP 프라이빗 클라우드의 통합 테스트

Secure Email 게이트웨이에서 연결을 테스트하는 직접적인 옵션은 없습니다. 로그 또는 경고를 검사하여 문제가 있는지 확인해야 합니다.

컨피그레이션은 AMP 검사를 시행하기 위해 보안 이메일 수신 메일 정책에서 수행됩니다.



Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	amp-testing-policy
Enable Advanced Malware Protection for This Policy:	◉ Enable File Reputation ☑ Enable File Analysis ○ Use Default Settings (AMP and File Analysis Enabled) ○ No
Message Scanning	
	☑ (recommended) Include an X-header with the AMP results in messages
Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is
▷ Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is
▷ Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is
▷ Advanced	Optional settings for custom header and message delivery.
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message
Archive Original Message:	○ No ◉ Yes
Drop Malware Attachments:	◉ No ○ Yes
Modify Message Subject:	○ No ◉ Prepend ○ Append [WARNING: MALWARE DETECTED]
▷ Advanced	*Optional settings.*
Messages with File Analysis Pending:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	○ No ◉ Yes
Drop Message Attachments with File Analysis Verdict Pending : ?	◉ No ○ Yes
Modify Message Subject:	○ No ◉ Prepend ○ Append [WARNING: ATTACHMENT(S) MAY CONTAIN
▷ Advanced	*Optional settings.*

비악성 파일로 ESA 테스트 CSV 파일입니다.

보안 이메일 mail_logs

```
Tue Feb 20 11:55:58 2024 Info: New SMTP ICID 43855 interface Management (10.106.39.193) address 10.110.172.122 reverse dns host unknown verified no
Tue Feb 20 11:55:58 2024 Info: ICID 43855 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918 country not applicable
Tue Feb 20 11:55:58 2024 Info: Start MID 660 ICID 43855
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 From: <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSCO-W-PF2S3NK0, env-from: gmail.com, header-from: Not Present, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 RID 0 To: <ajayra@cisco.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 Subject "testing amp private cloud"
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSCO-W-PF2S3NK0, env-from: gmail.com, header-from: gmail.com, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Tracker Header : 65d445f6_/TdY46k/XzoiL66+HhA4cFJoO192jJQ5DhlDLnEkX9DPCixVhxF3o31CI36to+TzXKqIaVVfPh6nXL+cND+SiQ==
Tue Feb 20 11:55:58 2024 Info: MID 660 ready 5467 bytes from <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 attachment 'Training Details.csv'
Tue Feb 20 11:55:58 2024 Info: MID 660 matched all recipients for per-recipient policy amp-testing-policy in the inbound table

Tue Feb 20 11:56:59 2024 Warning: graymail [RPC CLIENT] MID 660 Graymail scan timed out
Tue Feb 20 11:57:01 2024 Info: MID 660 AMP file reputation verdict : UNKNOWN(File analysis pending)
Tue Feb 20 11:57:01 2024 Info: MID 660 SHA 90381c261f8be3e9330710ab966473586c4514f6834c8ca0014d8e40dec4f19dbe filename Training Details.csv queued for possible file analysis upload
Tue Feb 20 11:57:01 2024 Info: MID 660 Outbreak Filters: verdict negative
Tue Feb 20 11:57:01 2024 Info: MID 660 Message-ID '<99221a3k@esa1.nanganath.local>'
Tue Feb 20 11:57:01 2024 Info: MID 660 queued for delivery
Tue Feb 20 11:57:01 2024 Info: New SMTP DCID 542 interface 10.106.39.193 address 173.37.147.230 port 25
Tue Feb 20 11:57:02 2024 Info: Delivery start DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: Message done DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: MID 660 RID [0] Response 'ok:  Message 142767851 accepted'
Tue Feb 20 11:57:04 2024 Info: Message finished MID 660 done
Tue Feb 20 11:57:09 2024 Info: DCID 542 close
Tue Feb 20 11:57:23 2024 Info: ICID 43855 lost
Tue Feb 20 11:57:23 2024 Info: ICID 43855 close
```

보안 이메일 AMP 로그

Tue Feb 20 11:57:01 2024 Info: Cloud에서 파일 평판 쿼리에 대한 응답을 받았습니다. 파일 이름 = Training Details.csv, MID = 660, Disposition = FILE UNKNOWN, Malware = None, Analysis Score = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload_action = 분석을 위해 파일을 보낼 것을 권장, verdict_source = AMP, suspected_categories = None

보안 엔드포인트 프라이빗 클라우드 이벤트 로그

{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":299
9277-4008-a396-
6cd486ecc621","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa:0,"fs:0","ft":0,"hd":1},"sha256":{"h":"

rd - 1개의 DISP_UNKNOWN입니다. 파일 속성을 알 수 없습니다.

통합이 실패하는 일반적인 문제가 발견됨

1. SWA 또는 보안 이메일에서 잘못된 "라우팅 테이블"을 선택합니다. 통합 디바이스는 AMP 프라이빗 클라우드 Eth1 인터페이스와 통신할 수 있어야 합니다.
2. VPC 호스트 이름은 SWA 또는 보안 이메일에서 DNS를 확인할 수 없으므로 연결 설정에 실패합니다.
3. VPC 속성 인증서의 CN(Common Name)은 SWA 및 Secure Email Gateway에 언급된 호스트 이름뿐만 아니라 VPC 호스트 이름과도 일치해야 합니다.
4. 프라이빗 클라우드와 클라우드 파일 분석을 사용하는 것은 지원되는 설계가 아닙니다. 온프레미스 디바이스를 사용하는 경우 파일 분석 및 평판은 온프레미스 서버여야 합니다.
5. AMP 프라이빗 클라우드와 SWA 보안 이메일 간에 시간 동기화 문제가 없는지 확인합니다.
6. SWA DVS 엔진 개체 검사 제한은 기본적으로 32MB입니다. 더 큰 파일을 스캔하려면 이 설정을 조정하십시오. 전역 설정이며 Webroot, Sophos 등 모든 스캐닝 엔진에 영향을 미칩니다.

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.