セキュアなエンドポイントプライベートクラウドとセキュアなWebおよび電子メールの統合

内容

はじめに

このドキュメントでは、セキュアエンドポイントプライベートクラウドをSecure Web Appliance(SWA)およびセキュアEメールゲートウェイ(ESA)と統合するために必要な手順について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

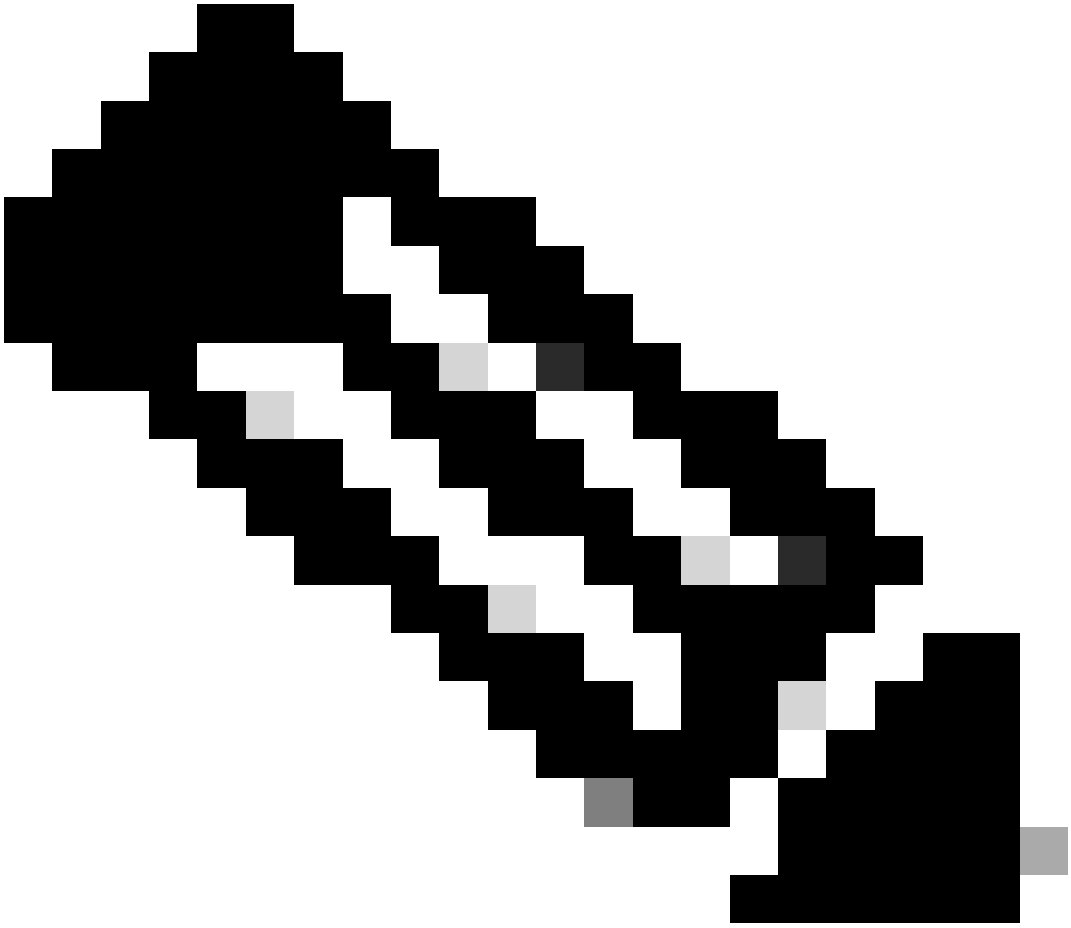
- セキュアエンドポイントAMP仮想プライベートクラウド
- セキュアWebアプライアンス(SWA)
- Secure Email Gateway

使用するコンポーネント

SWA（セキュアWebアプライアンス）15.0.0-322

AMP仮想プライベートクラウド4.1.0_202311092226

セキュアEメールゲートウェイ14.2.0-620



注：このドキュメントは、対象となるすべての製品の物理的および仮想的なバリエーションに対して有効です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

統合に進む前の検証チェック

1. が必要なライセンス **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** を持っているかどうかを確認します。機能キーを確認するか、またはスマートライセンスが有効になっているこ **SWA/Secure Email** とを確認できます。
2. HTTPSトラフィックの検査を計画している場合は、SWAでHTTPSプロキシを有効にする必要があります。ファイルレピュテーションチェックを行うには、HTTPSトラフィックを復号化する必要があります。
3. AMPプライベートクラウド/仮想プライベートクラウドアプライアンスと、必要なすべての

証明書を設定する必要があります。検証については、VPC証明書ガイドを参照してください。

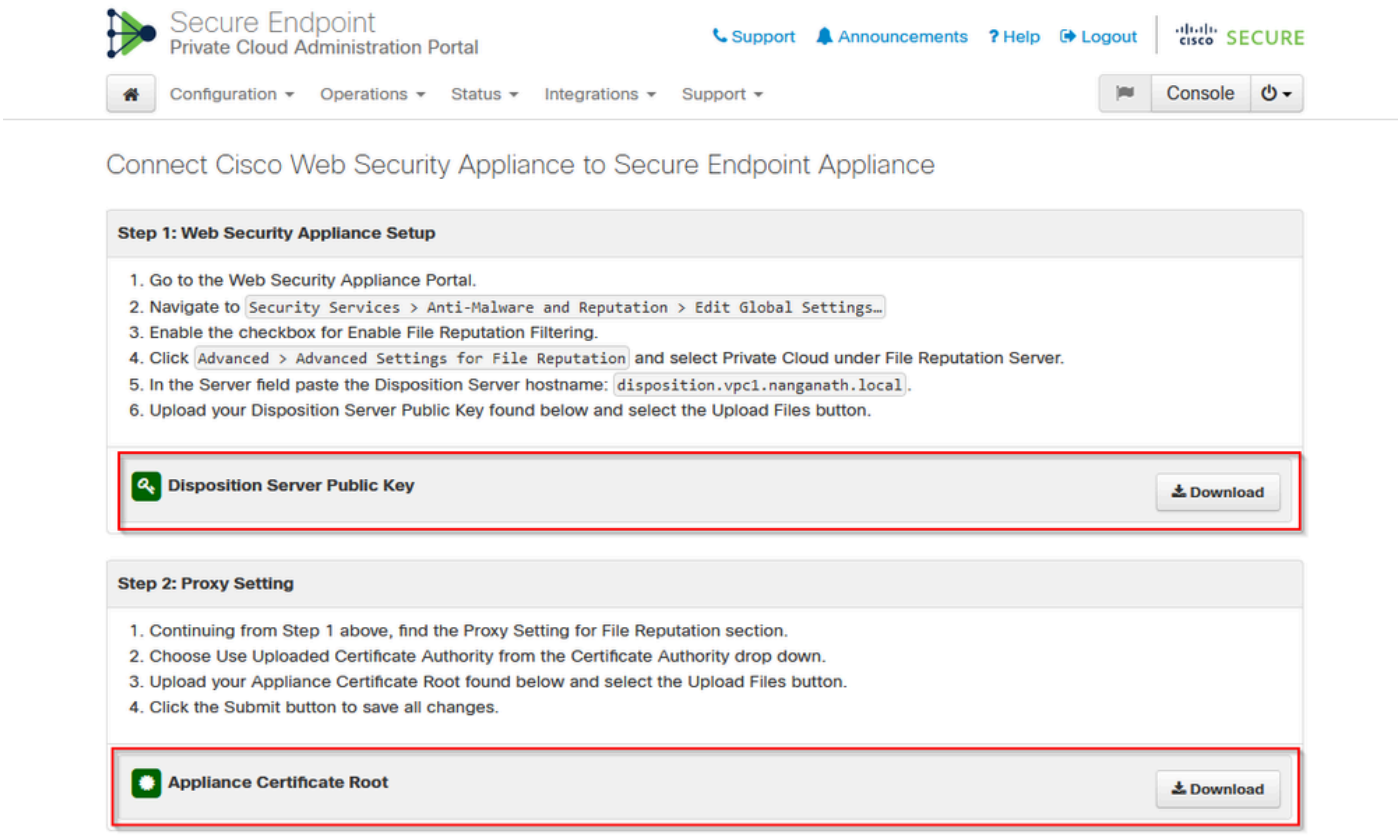
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html

4. 製品のすべてのホスト名は、DNSで解決できる必要があります。これは、統合中の接続の問題や証明書の問題を回避するためです。セキュアエンドポイントのプライベートクラウドでは、Eth0インターフェイスは管理者アクセス用であり、Eth1は統合デバイスに接続できる必要があります。

手順

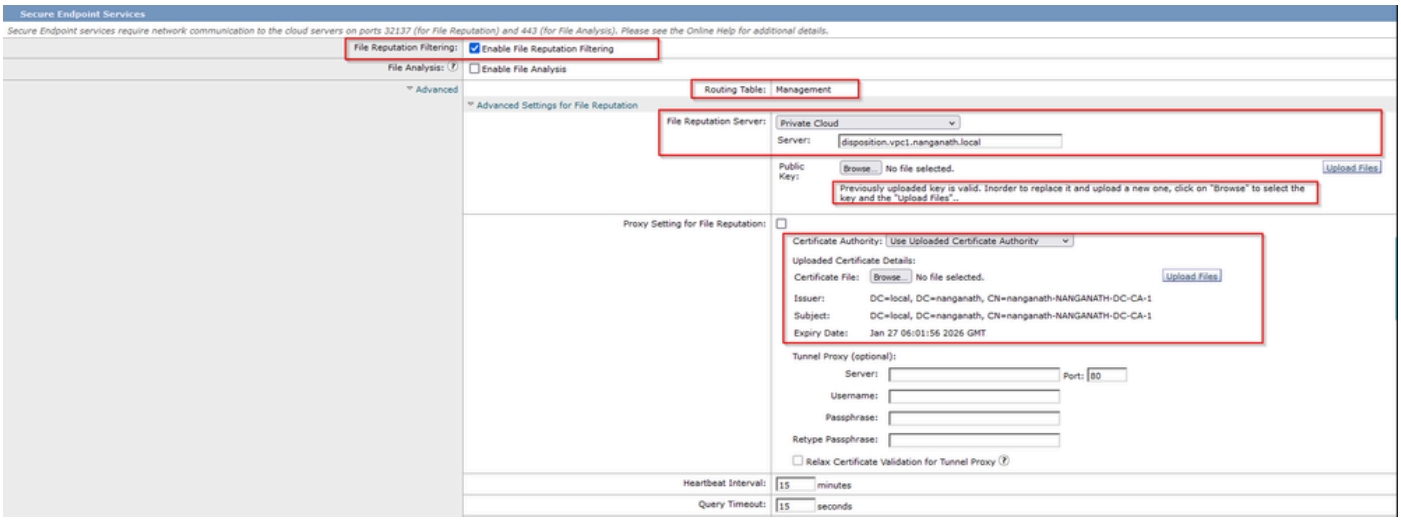
セキュアエンドポイントのプライベートクラウドの設定

1. **Secure Endpoint VPC admin portal**にログインします。
2. **“Configuration” > “Services” > “Disposition Server” >** Copy the disposition server hostnameに移動します（これは3番目のステップからフェッチすることもできます）。
3. **“Integrations” > “Web Security Appliance”**に移動します。
4. **“Disposition Server Public Key” & “Appliance Certificate Root”**をダウンロードします。
5. **“Integrations” > “Email Security Appliance”**に移動します。
6. ESAのバージョンを選択し、「Disposition Server Public Key」と「Appliance Certificate Root」をダウンロードします。
7. 証明書とキーの両方を安全に保管してください。これは、後でSWA/セキュアメールにアップロードする必要があります。



セキュアWebアプライアンスの設定

1. 移動先： **SWA GUI > “Security Services” > “Anti-Malware and Reputation” > Edit Global Settings**
2. 「Secure Endpoint Services」の下に「Enable File Reputation Filtering」オプションが表示され、「Check」このオプションには新しいフィールド「Advanced」が表示されます。
3. ファイルレピュテーションサーバで「プライベートクラウド」を選択します。
4. プライベートクラウドの評価サーバのホスト名を「サーバ」として指定します。
5. 以前にダウンロードした公開キーをアップロードします。「ファイルのアップロード」をクリックします。
6. 認証局をアップロードするオプションがあります。ドロップダウンから「Use Uploaded Certificate Authority」を選択し、以前にダウンロードしたCA証明書をアップロードします。
7. 変更を送信します
8. 変更を確定します



Cisco Secure Emailの設定

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

2. ファイルレピュテーションサーバで「プライベートクラウド」を選択します

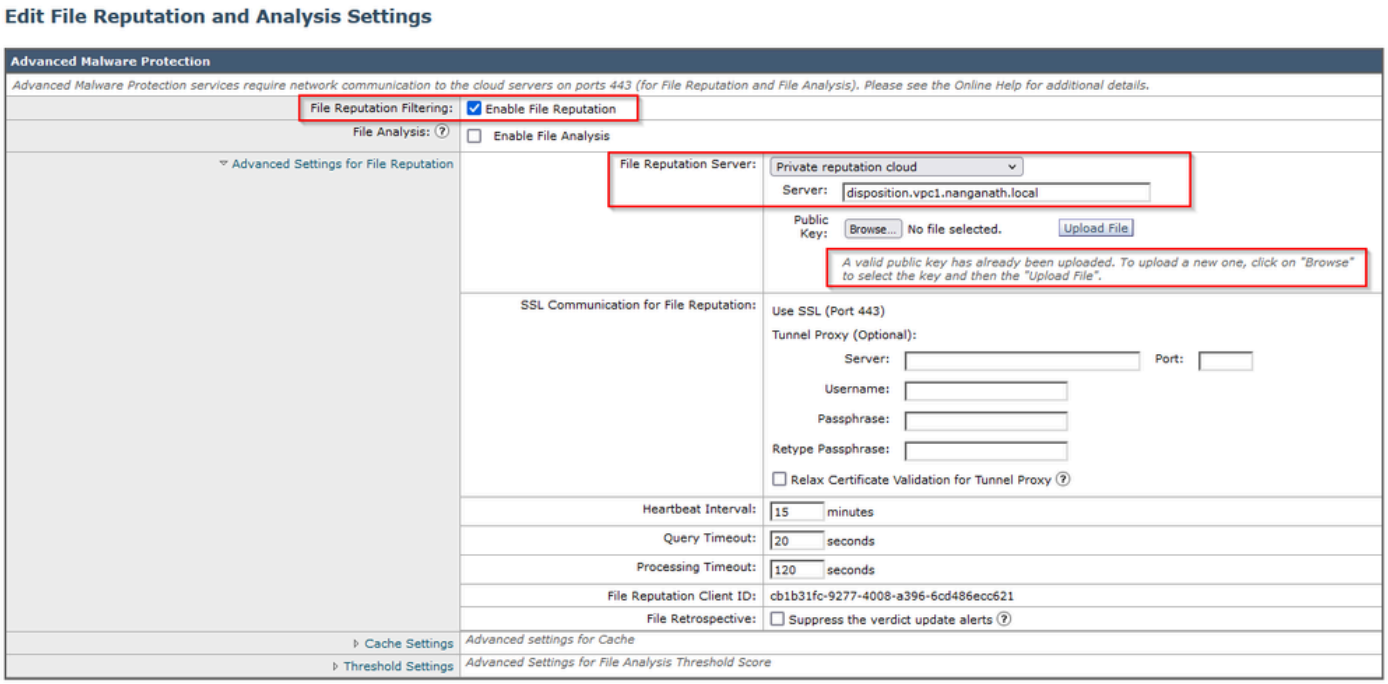
3. プライベートクラウドの評価サーバのホスト名を「サーバ」として指定します。

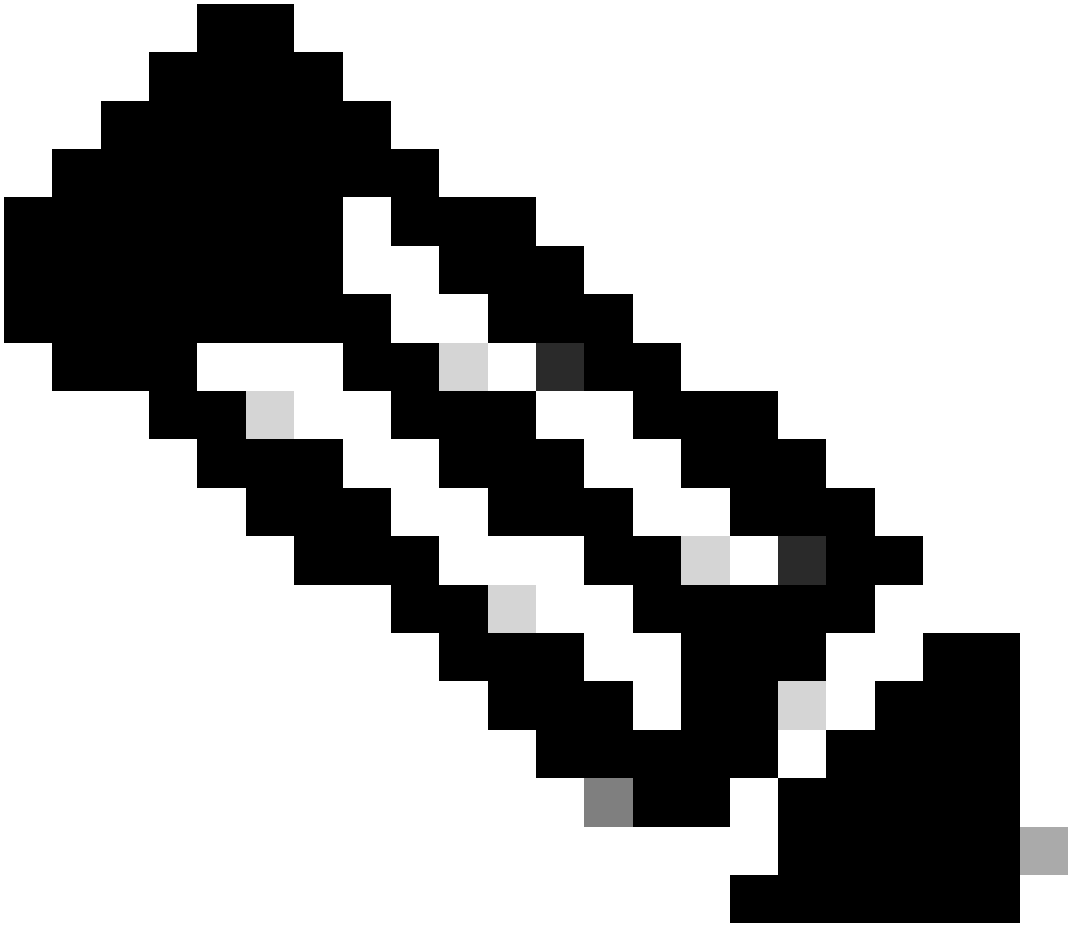
4. 前にダウンロードした公開キーをアップロードします。「ファイルのアップロード」をクリックします。

5. 認証局をアップロードします。ドロップダウンから「Use Uploaded Certificate Authority」を選択し、以前にダウンロードしたCA証明書をアップロードします。

6. 変更を送信します

7. 変更を確定します





注：Cisco Secure Web ApplianceおよびCisco Secure Email GatewayはAsyncOSをベースとしており、ファイルレピュテーションが初期化されるとほとんど同じログを共有します。AMPログは、セキュアWebアプライアンスまたはセキュアEメールゲートウェイAMPログ（両方のデバイスの同様のログ）で確認できます。これは、サービスがSWAおよびセキュアEメールゲートウェイで初期化されることを示しているだけです。接続が完全に成功したことを示すものではありません。接続または証明書の問題がある場合は、「ファイルレピュテーション初期化」メッセージの後にエラーが表示されます。ほとんどの場合、「到達不能エラー」または「証明書が無効」エラーを示します。

セキュアなWebおよび電子メールからAMPログを取得する手順

1. SWA/Secure Email Gateway CLIにログインし、コマンドを入力します。 **"grep"**

2. 選択 **"amp" or "amp_logs"**

3. その他のフィールドはそのままにして、ログの末尾に「Y」を入力します。ログの末尾にライブイベントが表示されます。古いイベントを探している場合は、「正規表現」に日付を入力でき

ます

```
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.
```

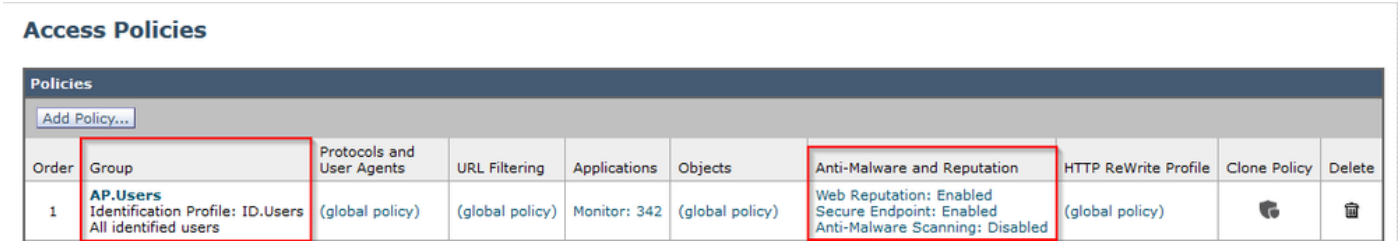
Secure Web ApplianceとSecure Endpointプライベートクラウド間の統合をテストしています。

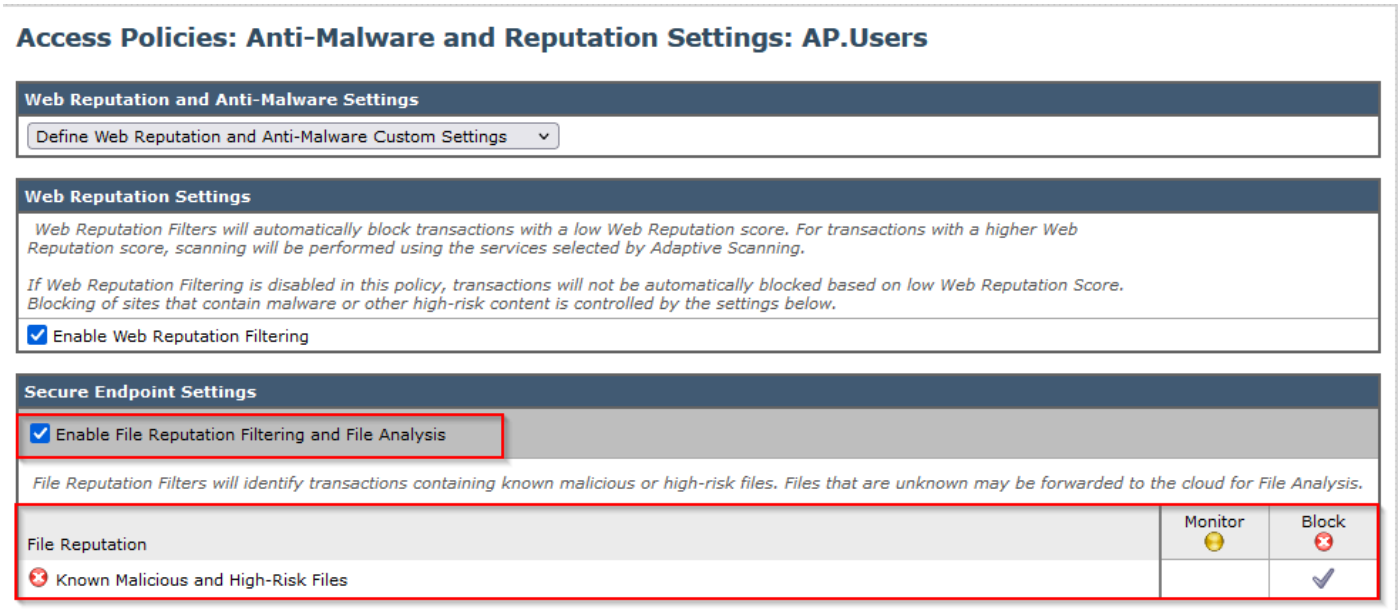
SWAからの接続を直接テストするオプションはありません。ログまたはアラートを調べて、問題があるかどうかを確認する必要があります。

説明を簡単にするため、ここではHTTPSではなくHTTP URLをテストしています。ファイルレピュテーションチェックのために、HTTPSトラフィックを復号化する必要があることに注意してください。

設定はSWAアクセスポリシーで行い、AMPスキャンを適用します。

注：Cisco Secure Web Applianceでのポリシーの設定方法については、SWAのユーザガイドを参照してください。





悪意のあるファイル「Bombermania.exe.zip」をCiscoセキュアWebアプライアンス経由でインターネットからダウンロードしようとしました。ログには、悪意のあるファイルがブロックされていることが示されています。

SWAアクセスログ

アクセスログは、次の手順で取得できます。

1. SWAにログインし、コマンドを入力します。 **"grep"**

2. 選択 **"accesslogs"**

3. クライアントIP等の「正規表現」を追加したい場合は言及すること。

4. ログの末尾に「Y」を入力

1708320236.640 61255 10.106.37.205 TCP_DENIED/403 2555785 GET 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-ID.Users-NONE-NONE-NONE-DefaultGroup-NONE <"IW_comp",3.7,1,"-",-,-,-,-,-, "-",1,-"-","-",-,-,"IW_comp",-,"AMP高リスク","コンピュータとインターネット","-","不明","不明","-","-",333.79,0,-,"-","-",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"Bombermania.exe.zip","46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8",3,-,"-",-,> -

TCP_DENIED/403 —> SWAがこのHTTP GET要求を拒否しました。

BLOCK_AMP_RESP —> AMP応答により、HTTP GET要求がブロックされました。

Win.Ransomware.Protected::Trojan.Agent.talos —>脅威名

Bombermania.exe.zip —>ダウンロードしようとしたファイル名

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 —>ファイルのSHA値

SWA AMPログ

AMPログは、次の手順を使用して取得できます。

1. SWAにログインし、コマンドを入力します。 **"grep"**

2. 選択 **"amp_logs"**

3. その他のフィールドはそのままにして、ログの末尾に「Y」を入力します。ログの末尾にライブイベントが表示されます。古いイベントを探している場合は、「正規表現」に日付を入力できます

「判定(verdict_from)」:「クラウド」。これはプライベートクラウドとパブリッククラウドで同じと思われます。判定とパブリッククラウドを混同しないでください。

2月19日（月）10:53:56 2024 Debug: Adjusted verdict - {'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', dict_source': None, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_reason': 'File type is not configured for sandboxing', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d8d8572f 31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicious_child': None}

セキュアエンドポイントプライベートクラウドのイベントログ

イベントログは、 **/data/cloud/log**

SHA256を使用するか、SWAの「ファイルレピュテーションクライアントID」を使用して、イベントを検索できます。ファイルレピュテーションクライアントIDは、SWAのAMP設定ページに表示されます。

pv：プロトコルバージョン、3はTCP

ip：このフィールドは、レピュテーションクエリーを実行したクライアントの実際のIPアドレスを示す保証がないため、このフィールドは無視してください

uu:WSA/ESA内のファイルレピュテーションクライアントID

SHA256 – ファイルのSHA256

dn：検出名

n - AMPでファイルハッシュがこれまでに検出されたことがない場合は1、それ以外の場合は0。

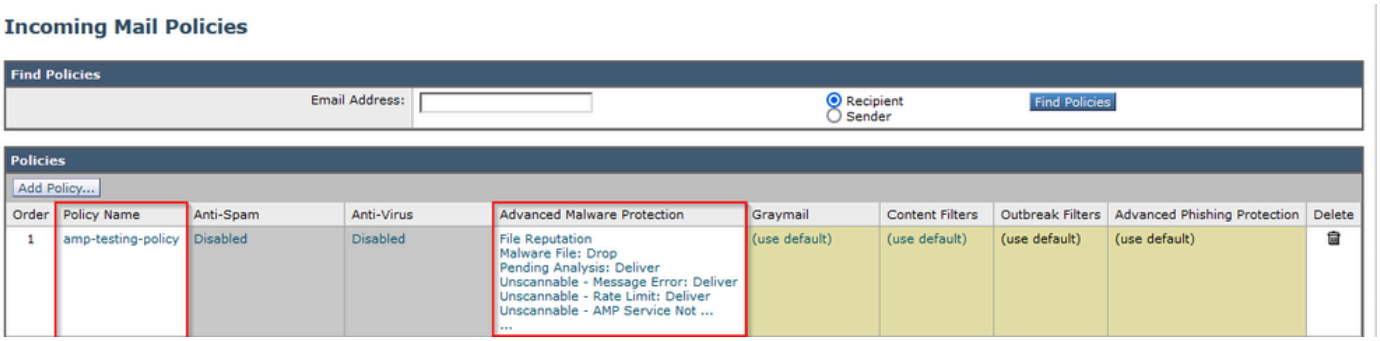
rd:Response Disposition。ここで、3はDISP_MALICIOUSを意味します。

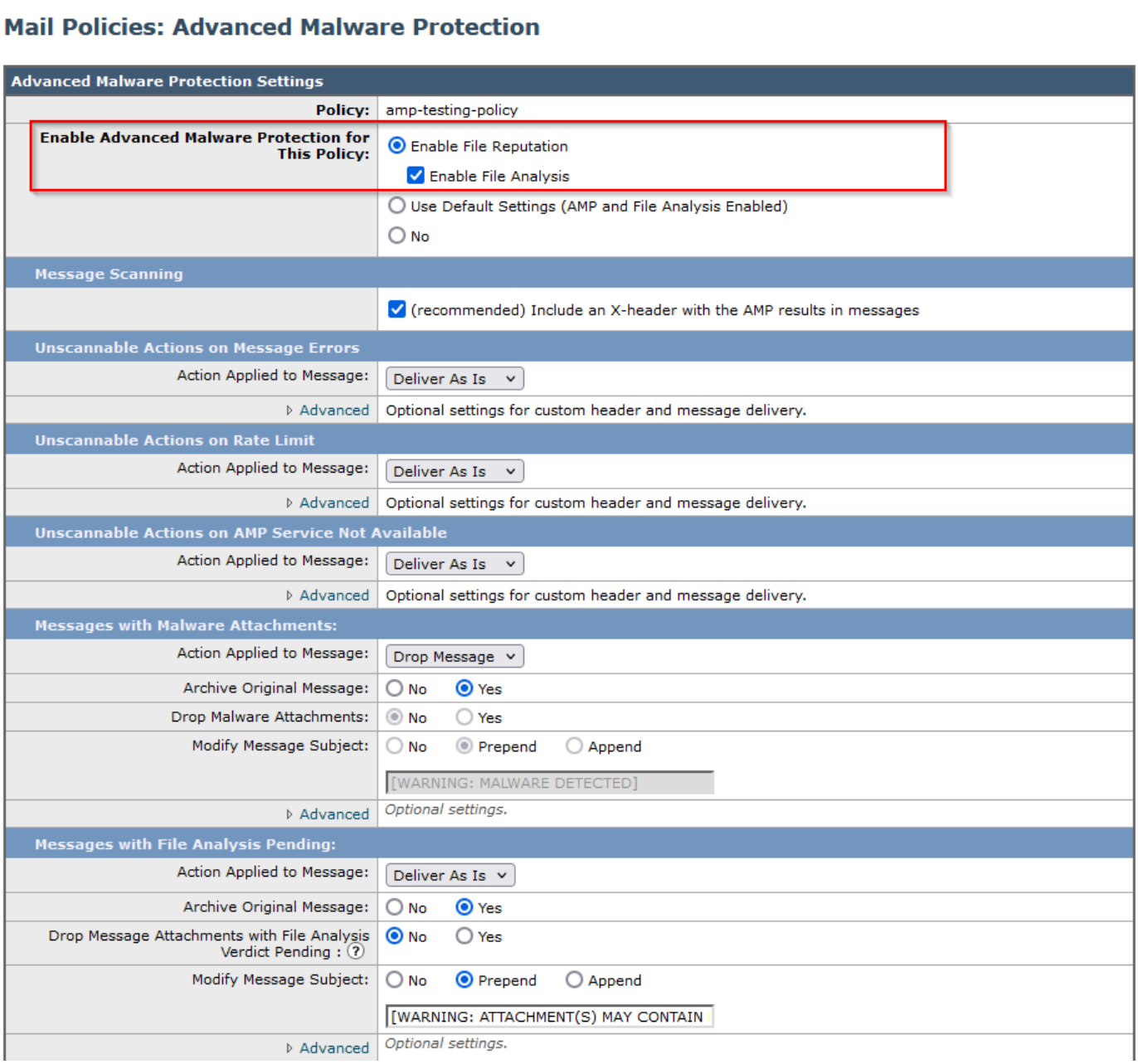
1 DISP_UNKNOWNファイルの性質が不明です。
2 DISP_CLEANファイルは良性であると考えられます。
3 DISP_MALICIOUSファイルは悪意があると考えられています。
7 DISP_UNSEENファイルの性質が不明で、ファイルを初めて見た時です。
13 DISP_BLOCKファイルは実行できません。
14 DISP_IGNORE XXX
15 DISP_CLEAN_PARENTファイルは無害であると考えられ、作成される悪意のあるファイルはunknownとして扱われる必要があります。
16 DISP_CLEAN_NFMファイルは良性であると考えられますが、クライアントはネットワークトラフィックを監視する必要があります。

セキュアな電子メールとAMPプライベートクラウド間の統合のテスト

セキュアEメールゲートウェイからの接続をテストする直接のオプションはありません。ログまたはアラートを調べて、問題があるかどうかを確認する必要があります。

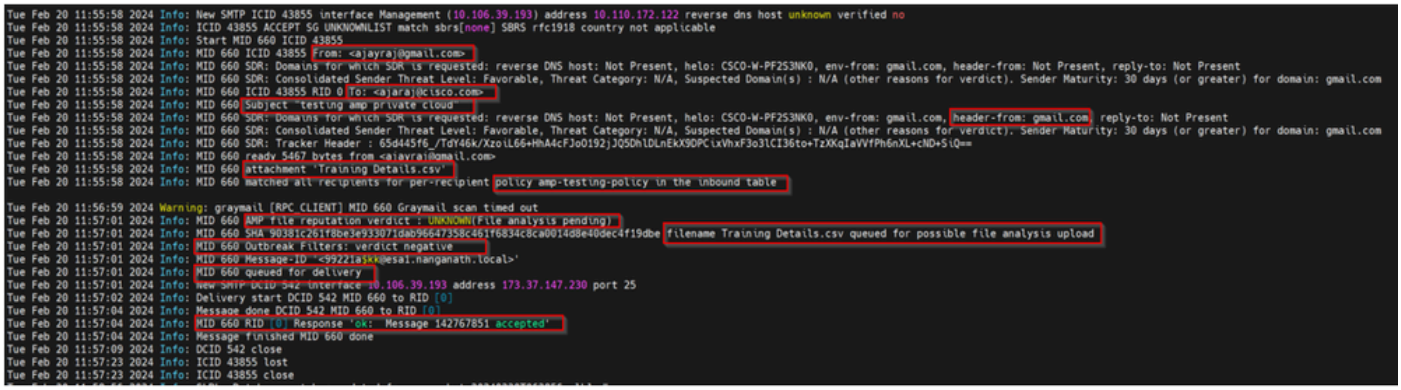
設定は、AMPスキャンを適用するためにセキュアメールの着信メールポリシーで行われます。





悪意のないファイルを使用してESAをテスト。これはCSVファイルです。

セキュリティで保護された電子メールのログ



セキュアな電子メールAMPログ

2月20日（火）11:57:01 2024情報：ファイルレピュテーションクエリに対する応答をクラウドから受信しました。File Name = Training Details.csv、MID = 660、Disposition = FILE UNKNOWN、マルウェア=なし、分析スコア= 0、sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe、upload_action =分析用にファイルを送信することを推奨、verdict_source = AMP、suspected_categories =なし

セキュアエンドポイントプライベートクラウドのイベントログ

{"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":"90381C261F8B
f19DBE","fa":0,"fs":0,"ft":0,"hd":1},"hold":[32,4],"rd":1,"ra":1,"n":0}

rd - 1 DISP_UNKNOWN。ファイルの性質が不明です。

統合障害の原因となる一般的な問題

1. SWAまたはセキュアメールで誤った「ルーティングテーブル」を選択する。統合デバイスは、AMPプライベートクラウドEth1インターフェイスと通信できる必要があります。
2. VPCホスト名がSWAまたはセキュアメールでDNS解決できないため、接続の確立に失敗します。
3. VPCディスポジション証明書のCN（共通名）は、VPCホスト名だけでなく、SWAおよびセキュアEメールゲートウェイで説明したものと一致する必要があります。
4. プライベートクラウドとクラウドファイル分析の使用は、サポートされている設計ではありません。オンプレミスデバイスを使用している場合、ファイル分析とレピュテーションはオンプレミスサーバである必要があります。
5. AMPプライベートクラウドとSWA間の時間同期の問題、セキュアな電子メールがないことを確認します。
6. SWA DVSエンジンのオブジェクトスキャン制限は、デフォルトで32 MBに設定されています。より大きなファイルをスキャンする場合は、この設定を調整します。これはグローバル設定であり、WebrootやSophosなどのすべてのスキャンエンジンに影響することに注意してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。