Integration einer sicheren Endpunkt-Private-Cloud mit sicherem Web und E-Mail

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Integration der Secure Endpoint Private Cloud in die Secure Web Appliance (SWA) und Secure Email Gateway (ESA) beschrieben.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

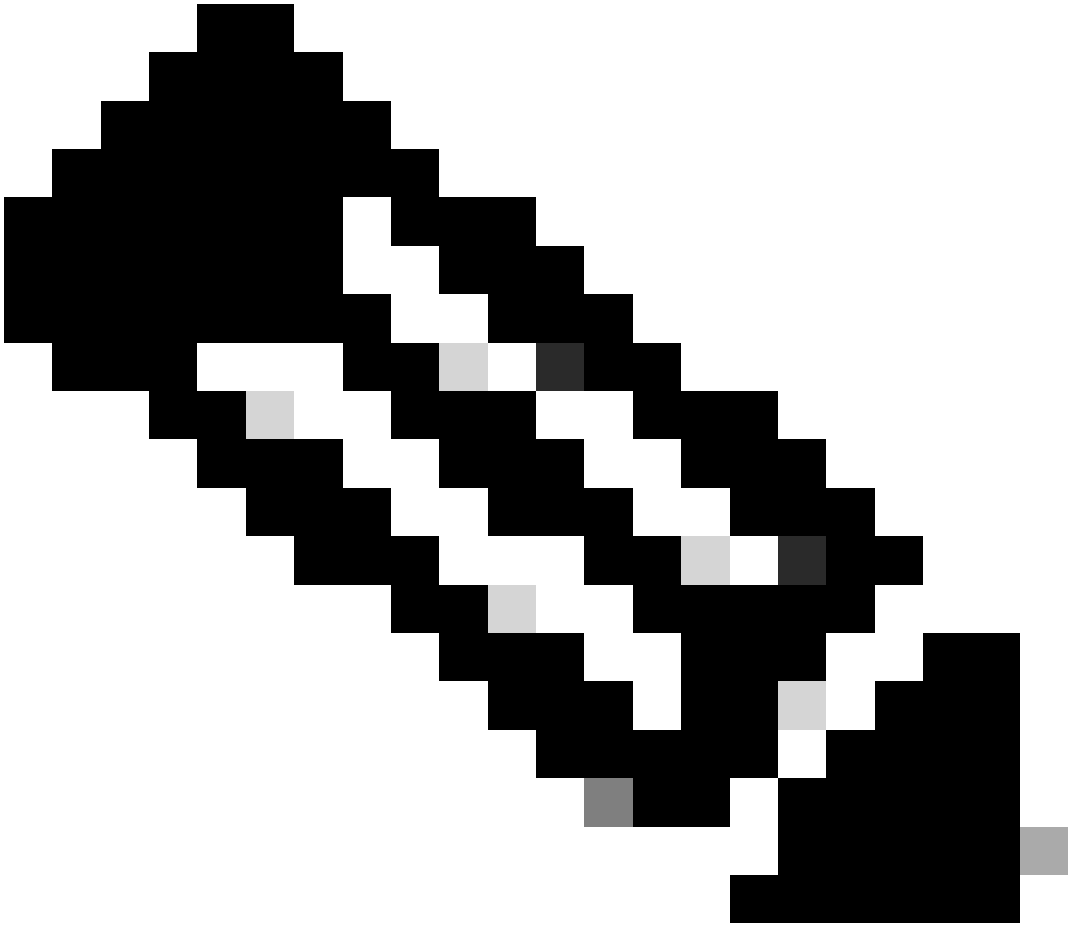
- Sichere Endpunkt-AMP Virtual Private Cloud
- Secure Web Appliance (SWA)
- Sicheres E-Mail-Gateway

Verwendete Komponenten

SWA (Secure Web Appliance) 15.0.0-322

AMP Virtual Private Cloud 4.1.0_202311092226

Sicheres E-Mail-Gateway 14.2.0-620



Hinweis: Die Dokumentation gilt für physische und virtuelle Varianten aller beteiligten Produkte.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Verifizierungsprüfungen vor der Integration

1. Überprüfen Sie, ob **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** die erforderlichen Lizenzen vorhanden sind. Sie können den Feature-Schlüssel überprüfen oder **SWA/Secure Email** überprüfen, ob die Smart-Lizenz aktiviert ist.
2. HTTPS-Proxy muss auf SWA aktiviert sein, wenn Sie den HTTPS-Datenverkehr überprüfen möchten. Sie müssen den HTTPS-Datenverkehr entschlüsseln, um die Dateireputationsprüfung durchführen zu können.
3. Die AMP Private Cloud/Virtual Private Cloud-Appliance und alle erforderlichen Zertifikate

müssen konfiguriert werden. Weitere Informationen zur Verifizierung finden Sie im VPC-Zertifikatsleitfaden.

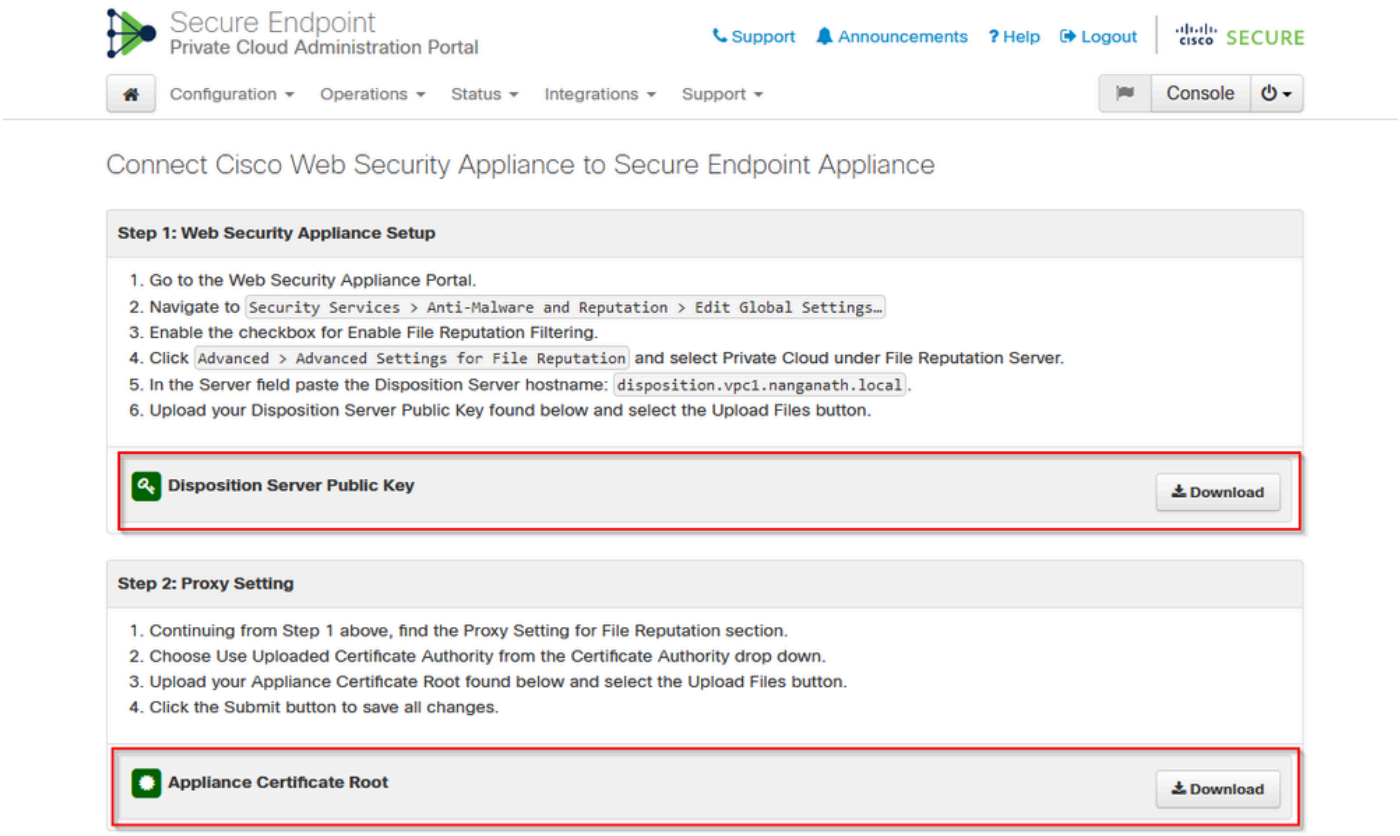
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html

4. Alle Hostnamen der Produkte müssen in DNS auflösbar sein. Auf diese Weise sollen Verbindungsprobleme oder Zertifizierungsprobleme bei der Integration vermieden werden. In der Secure Endpoint Private Cloud ist die Eth0-Schnittstelle für den Administratorzugriff vorgesehen, und Eth1 muss in der Lage sein, eine Verbindung mit integrierenden Geräten herzustellen.

Vorgehensweise

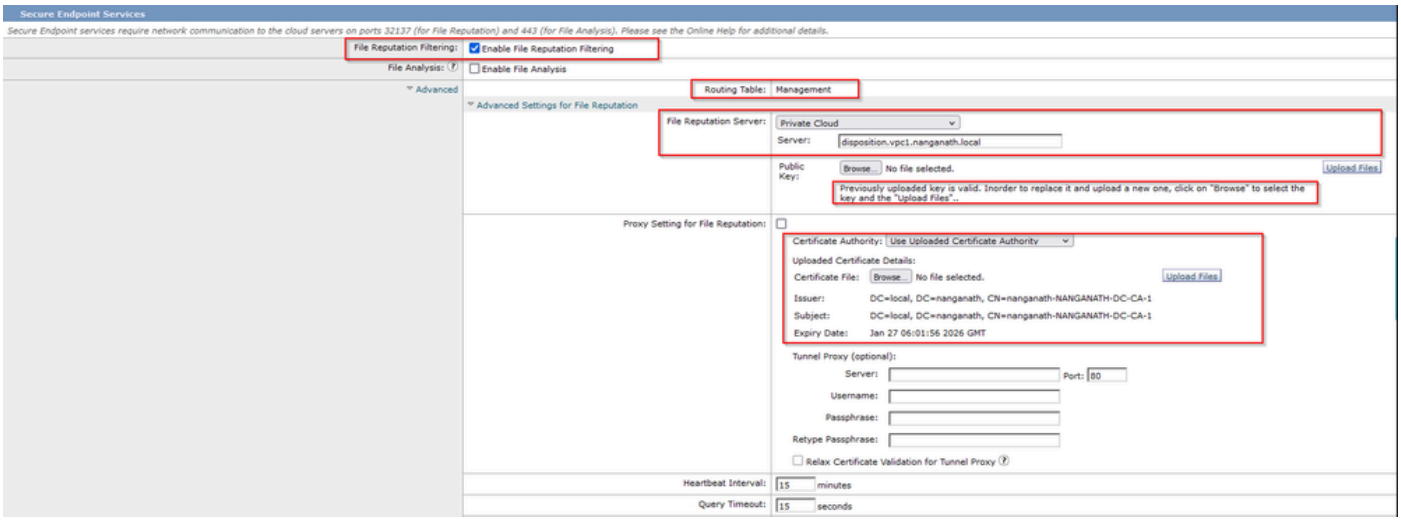
Konfigurieren der Secure Endpoint Private Cloud

1. Melden Sie sich beim **Secure Endpoint VPC admin portal**an.
2. Gehen Sie zu **“Configuration”** > **“Services”** > **“Disposition Server”** > Kopieren Sie den Hostnamen des Dispositionsservers (dies kann auch aus dem dritten Schritt geholt werden).
3. Navigieren Sie zu .**“Integrations”** > **“Web Security Appliance”**
4. Laden Sie die herunter **“Disposition Server Public Key” & “Appliance Certificate Root”** .
5. Navigieren Sie zu .**“Integrations”** > **“Email Security Appliance”**
6. Wählen Sie die Version Ihrer ESA aus, und laden Sie die Dateien "Disposition Server Public Key" und "Appliance Certificate Root" herunter.
7. Bitte bewahren Sie sowohl das Zertifikat als auch den Schlüssel auf. Diese muss zu einem späteren Zeitpunkt in SWA/Secure Email hochgeladen werden.



Konfigurieren der sicheren Web-Appliance

1. Navigieren Sie zu **SWA GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings**
2. Unter dem Abschnitt "Secure Endpoint Services" können Sie die Option "Enable File Reputation Filtering" sehen, und "Check" diese Option zeigt ein neues Feld "Advanced"
3. Wählen Sie im Datei-Reputationsserver "Private Cloud" aus.
4. Geben Sie als Hostnamen des Private Cloud Disposition Servers "Server" an.
5. Laden Sie den öffentlichen Schlüssel hoch, den Sie zuvor heruntergeladen haben. Klicken Sie auf "Dateien hochladen".
6. Es gibt eine Option zum Hochladen der Zertifizierungsstelle. Wählen Sie im Dropdown-Menü die Option "Use Uploaded Certificate Authority" (Hochgeladene Zertifizierungsstelle verwenden), und laden Sie das zuvor heruntergeladene Zertifizierungsstellenzertifikat hoch.
7. Änderungen übermitteln
8. Änderungen bestätigen



Konfigurieren der sicheren Cisco E-Mail

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

2. Wählen Sie "Private Cloud" im Datei-Reputationsserver

3. Geben Sie als Hostnamen des Private Cloud Disposition Servers "Server" an.

4. Laden Sie den öffentlichen Schlüssel hoch, den wir zuvor heruntergeladen haben. Klicken Sie auf "Dateien hochladen".

5. Laden Sie die Zertifizierungsstelle hoch. Wählen Sie im Dropdown-Menü die Option "Use Uploaded Certificate Authority" (Hochgeladene Zertifizierungsstelle verwenden), und laden Sie das zuvor heruntergeladene Zertifizierungsstellenzertifikat hoch.

6. Senden Sie die Änderung

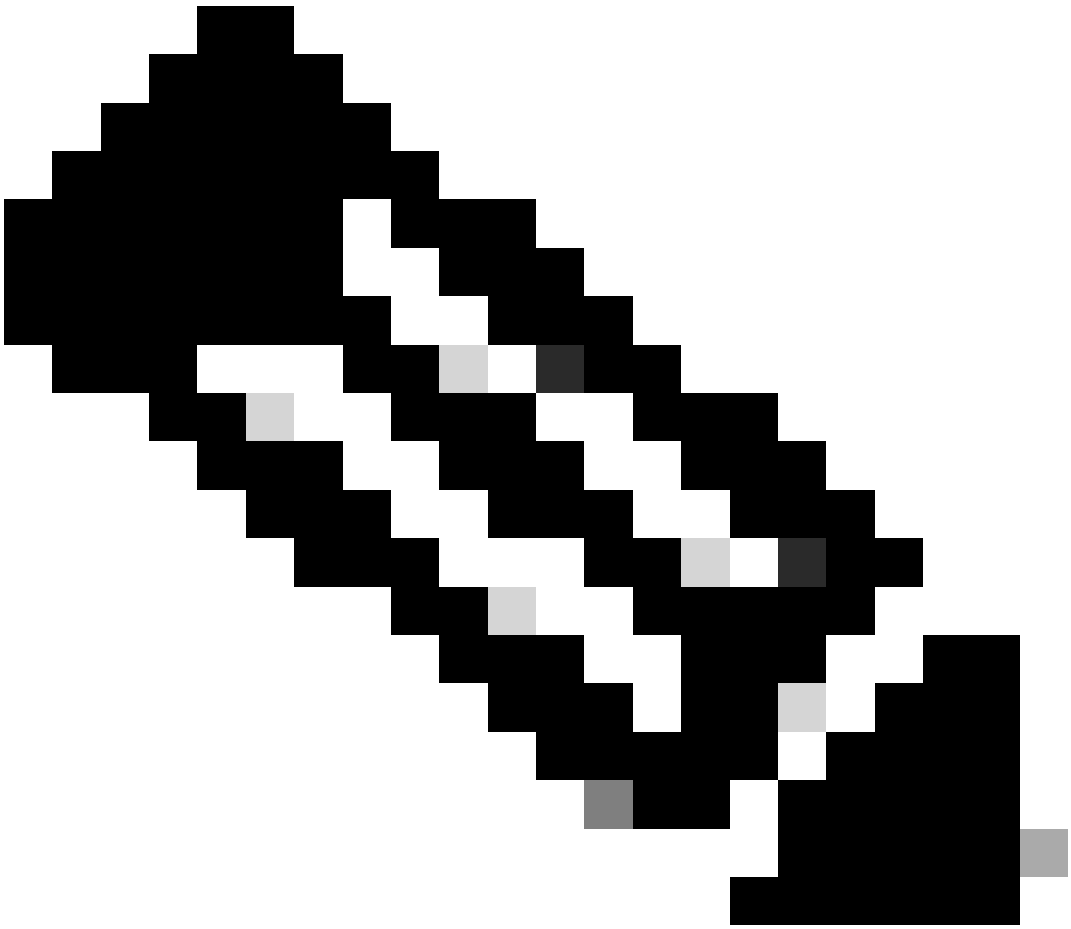
7. Bestätigen Sie die Änderung

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*



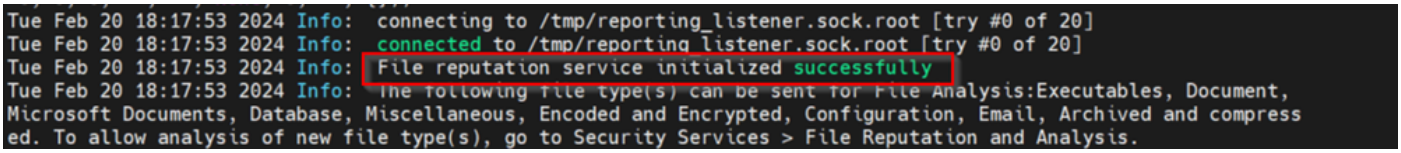
Hinweis: Die Cisco Secure Web Appliance und das Cisco Secure Email Gateway basieren auf AsyncOS und verwenden bei der Initialisierung der Dateireputation fast die gleichen Protokolle. Das AMP-Protokoll kann in AMP-Protokollen der sicheren Web-Appliance oder des sicheren E-Mail-Gateways angezeigt werden (ähnliche Protokolle in beiden Geräten). Dies zeigt nur an, dass der Dienst auf dem SWA und Secure Email Gateway initialisiert ist. Es gab keinen Hinweis darauf, dass die Verbindung vollständig erfolgreich war. Wenn Verbindungs- oder Zertifikatprobleme auftreten, werden nach der Meldung "File Reputation initialized" (Dateireputation initialisiert) Fehler angezeigt. Meist wird ein "Unreachable error" (Nicht erreichbarer Fehler) oder "certificate Invalid" (Ungültiges Zertifikat) angezeigt.

Schritte zum Abrufen von AMP-Protokollen aus sicheren Web- und E-Mail-Anwendungen

1. Melden Sie sich bei der CLI des SWA/Secure Email Gateway an, und geben Sie den Befehl **"grep"**

2. Wählen **"amp" or "amp_logs"**

3. Lassen Sie alle anderen Felder unverändert, und geben Sie "Y" ein, um die Protokolle zu verfolgen. Führen Sie die Protokolle durch, um die Live-Ereignisse anzuzeigen. Wenn Sie nach alten Ereignissen suchen, können Sie das Datum in "regulärer Ausdruck" eingeben



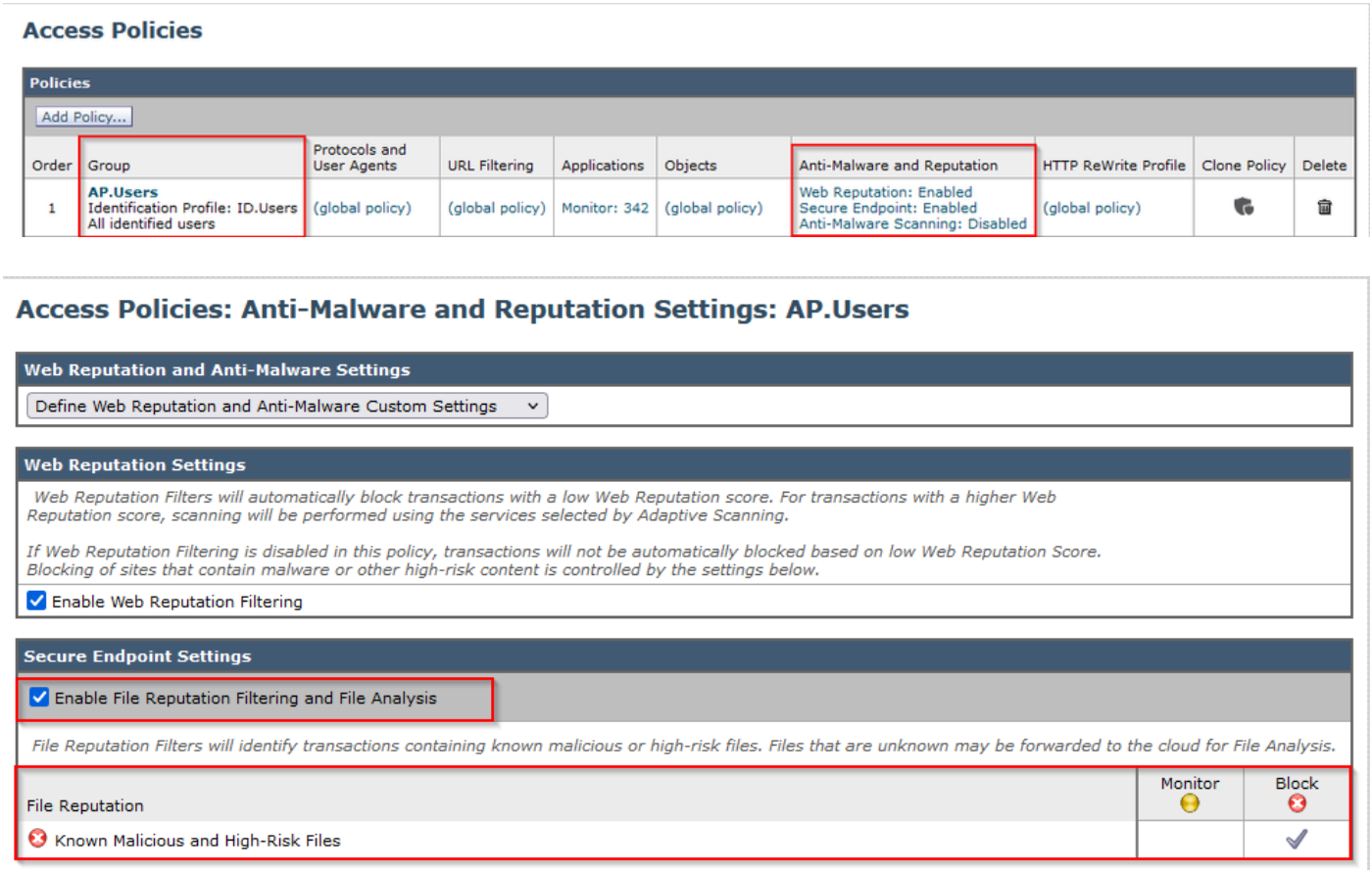
Test der Integration zwischen Secure Web Appliance und Secure Endpoint Private Cloud

Es gibt keine direkte Option zum Testen der SWA-Verbindung. Sie müssen die Protokolle oder Warnungen überprüfen, um festzustellen, ob Probleme vorliegen.

Der Einfachheit halber testen wir eine HTTP-URL anstelle von HTTPS. Beachten Sie, dass Sie den HTTPS-Datenverkehr für alle Dateireputationsprüfungen entschlüsseln müssen.

Die Konfiguration erfolgt in der SWA-Zugriffsrichtlinie und wird durch den AMP-Scan erzwungen.

Hinweis: Lesen Sie das SWA-Benutzerhandbuch, um zu erfahren, wie Sie die Richtlinien auf der Cisco Secure Web Appliance konfigurieren.



Es wurde versucht, eine schädliche Datei "Bombermania.exe.zip" über die sichere Web-Appliance von Cisco aus dem Internet herunterzuladen. Das Protokoll zeigt an, dass die schädliche Datei BLOCKIERT ist.

SWA-Zugriffsprotokolle

Die Zugriffsprotokolle können mit diesen Schritten abgerufen werden.

1. Melden Sie sich bei der SWA an, und geben Sie den Befehl **"grep"**

2. Wählen **"accesslogs"**

3. Wenn Sie einen "regulären Ausdruck" wie Client-IP hinzufügen möchten, erwähnen Sie diesen bitte.

4. Geben Sie "Y" ein, um das Protokoll zu verfolgen.

1708320236.640 61255 10.106.37.2015 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,"-",-,-,-,"-","-",1,-","-","-",-,-,-","IW_comp",-,"AMP hohes Risiko","Computer und Internet","-","Unbekannt","Unbekannt","-","-",333 .79,0,-,"-","-",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"Bombermania.exe.zip","46ee42fb79a161bf376","-","-,-> -

TCP_DENIED/403 —> SWA hat diese HTTP GET-Anforderung abgelehnt.

BLOCK_AMP_RESP —> Die HTTP GET-Anforderung wurde aufgrund der AMP-Antwort blockiert.

Win.Ransomware.Protected::Trojan.Agent.talos —> Name der Bedrohung

Bombermania.exe.zip —> Dateiname, den wir herunterladen wollten

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 —> SHA-Wert der Datei

SWA AMP-Protokolle

Die AMP-Protokolle können mit diesen Schritten abgerufen werden.

1. Melden Sie sich bei der SWA an, und geben Sie den Befehl **"grep"**

2. Wählen **"amp_logs"**

3. Lassen Sie alle anderen Felder unverändert, und geben Sie "Y" ein, um die Protokolle zu verfolgen. Führen Sie die Protokolle durch, um die Live-Ereignisse anzuzeigen. Wenn Sie nach alten Ereignissen suchen, können Sie das Datum in "regulärer Ausdruck" eingeben

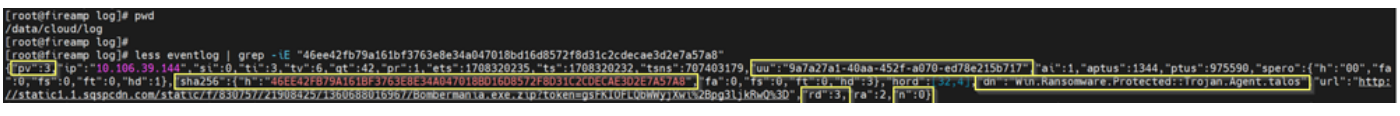
'verdict_from': 'Cloud' Dies scheint für Private Cloud und Public Cloud identisch zu sein. Verwechseln Sie es nicht mit einem Verdict aus der Public Cloud.

Mon Feb 19 10:53:56 2024 Debug: Adjusted verdict - {'category': 'amp', 'spyname': 'Win.Ransomware.Protected::Trojan.Agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status': 1 8, 'verdict_num': 3, 'analysis_score': 0, 'uploaded': False, 'file_name': 'Bombermania.exe.zip', 'verdict_source': Keine, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': application/zip', 'score': 0, 'upload_reason': 'Dateityp ist nicht für Sandboxing konfiguriert', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'BÖSWILLIG', 'bösartiges_Kind': Keine}

Private Cloud-Ereignisprotokolle für sichere Endgeräte

Die Ereignisprotokolle finden Sie unter **/data/cloud/log**

Sie können das Ereignis entweder mit dem SHA256 oder mit der "File Reputation Client ID" des SWA suchen. "File Reputation Client ID" (Dateireputations-Client-ID) ist auf der AMP-Konfigurationsseite des SWA vorhanden.



pv - Protokollversion, 3 steht für TCP

ip - Bitte ignorieren Sie dieses Feld, da es keine Garantie dafür gibt, dass dieses Feld die

tatsächliche IP-Adresse des Clients angibt, der die Reputationsabfrage durchgeführt hat.

uu - Dateireputations-Client-ID in WSA/ESA

SHA256 - SHA256 der Datei

dn - Der Erkennungsname

n - 1, wenn der Datei-Hash noch nie zuvor von AMP gesehen wurde, andernfalls 0.

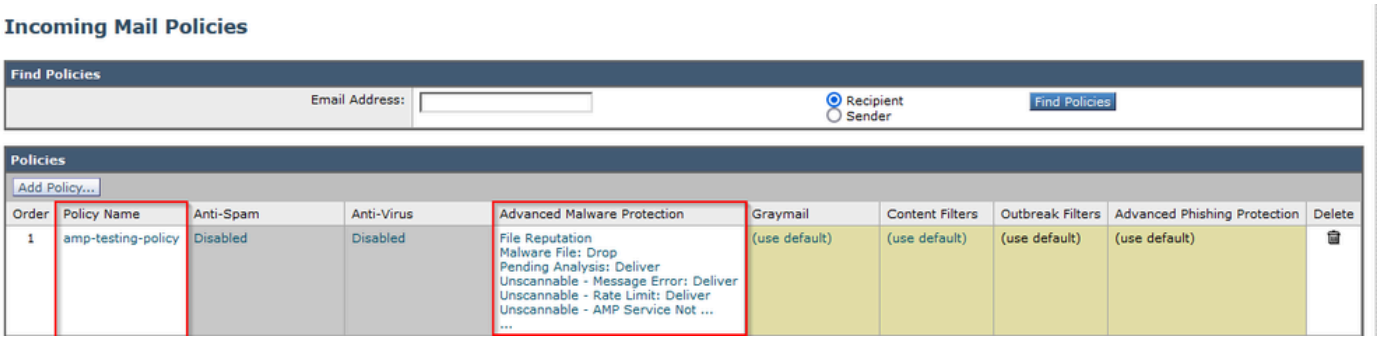
rd - Response Disposition. hier bedeutet 3 DISP_MALICIOUS

1 DISP_UNKNOWN Der Status der Datei ist unbekannt.
2 DISP_CLEAN Die Datei wird als harmlos angesehen.
3 DISP_MALICIOUS Die Datei ist vermutlich schädlich.
7 DISP_UNSEEN Der Dateistatus ist unbekannt und es ist das erste Mal, dass wir die Datei sehen.
13 DISP_BLOCK Die Datei darf nicht ausgeführt werden.
14 DISP IGNORIEREN XXX
15 DISP_CLEAN_PARENT Die Datei gilt als unbedenklich, und alle von ihr erstellten schädlichen Dateien müssen als unbekannt behandelt werden.
16 DISP_CLEAN_NFM Die Datei wird als harmlos angesehen, aber der Client muss den Netzwerkverkehr überwachen.

Test der Integration von Secure Email und AMP Private Cloud

Es gibt keine direkte Option zum Testen der Verbindung vom sicheren E-Mail-Gateway aus. Sie müssen die Protokolle oder Warnungen überprüfen, um festzustellen, ob Probleme vorliegen.

Die Konfiguration erfolgt in der Richtlinie für sichere eingehende E-Mails, um den AMP-Scan durchzusetzen.



Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	amp-testing-policy
Enable Advanced Malware Protection for This Policy:	(•) Enable File Reputation [x] Enable File Analysis ( ) Use Default Settings (AMP and File Analysis Enabled) ( ) No
Message Scanning	
	[x] (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.*

ESA mit einer nicht bösartigen Datei getestet. Dies ist eine CSV-Datei.

Sichere E-Mail-Protokolle

```
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 90181c261f8be3e9330710ab966473586c4619f6834c8ca0014d8e40dec4f19dbe 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
```

Sichere E-Mail-AMP-Protokolle

Di Feb 20 11:57:01 2024 Info: Antwort erhalten für Dateireputations-Abfrage von Cloud. Dateiname = Trainingsdetails.csv, MID = 660, Disposition = FILE UNKNOWN, Malware = None, Analysewert = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload_action = Empfohlen, um die Datei zur Analyse zu senden, verdict_source = AMP, suspied_categories = Keine

Secure Endpoint Private Cloud-Ereignisprotokolle

{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":299
"cb1b31fc-9277-4008-a396-6cd486ecc621","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":
F19DBE","fa":0,"fs":0,"ft":0,"hd":1},"hord":[32,4],"rd":1,"ra":1,"n":0}

rd - 1 DISP_UNKNOWN Der Dateistatus ist unbekannt.

Häufige Probleme, die zu Integrationsfehlern führen

1. Auswahl der falschen "Routing-Tabelle" in SWA oder Secure Email. Das integrierte Gerät muss mit der AMP Private Cloud Eth1-Schnittstelle kommunizieren können.
2. Der VPC-Hostname kann in SWA oder Secure Email nicht in DNS aufgelöst werden, was zu Fehlern beim Herstellen der Verbindung führt.
3. Der CN (Common Name) im VPC-Dispositionszertifikat muss mit dem VPC-Hostnamen sowie mit dem in SWA und Secure Email Gateway angegebenen Hostnamen übereinstimmen.
4. Die Verwendung einer Private Cloud und einer Cloud-Dateianalyse wird nicht unterstützt. Wenn Sie ein Gerät vor Ort verwenden, müssen die Dateianalyse und die Reputation ein Server vor Ort sein.
5. Stellen Sie sicher, dass es kein Problem mit der Zeitsynchronisierung zwischen der AMP Private Cloud und der SWA Secure Email gibt.
6. Der Objektscannergrenzwert des SWA-DVS-Moduls ist standardmäßig auf 32 MB festgelegt. Passen Sie diese Einstellung an, wenn Sie größere Dateien scannen möchten. Beachten Sie, dass es sich um eine globale Einstellung handelt, die alle Scan-Engines wie Webroot, Sophos usw. betrifft.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.