Bestandsanalyse uploads op ESA controleren

Inhoud

Inleiding

Dit document beschrijft hoe te bepalen of bestanden die worden verwerkt via Advanced Malware Protection (AMP) op de Cisco Email Security Appliance (ESA) worden verzonden voor bestandsanalyse, en ook wat het gekoppelde AMP-logbestand biedt.

Bepaal of er Attachments zijn geüpload voor bestandsanalyse

Als File Analysis is ingeschakeld, kunnen bijlagen die worden gescand met File Reputation naar File Analysis worden verzonden voor nadere analyse. Dit biedt het hoogste niveau van bescherming tegen bedreigingen met nul dagen en gerichte bedreigingen. Bestandsanalyse is alleen beschikbaar wanneer Filtering voor uploaden van bestanden is ingeschakeld.

Gebruik de opties Bestandstypen om de typen bestanden te beperken die naar de cloud kunnen worden verzonden. De specifieke bestanden die worden verzonden zijn altijd gebaseerd op verzoeken van de Cloud voor bestandanalyse, die zich richt op de bestanden waarvoor extra analyse nodig is. Bestandsanalyse voor bepaalde bestandstypen kan tijdelijk worden uitgeschakeld wanneer de cloud voor bestandanalyse capaciteit bereikt.

> Opmerking: Raadpleeg de Bestandscriteria voor geavanceerde Malware Protection Services voor Cisco Content Security Producten Cisco-document voor de meest actuele en extra informatie.

> Opmerking: Controleer de Releaseopmerkingen en de gebruikersgids voor de specifieke herziening van AsyncOS die op uw apparaat draait, omdat de bestandstypen voor bestandanalyse kunnen verschillen afhankelijk van de versie van AsyncOS.

Bestandstypen die voor bestandsanalyse kunnen worden verzonden:

- De volgende bestandstypen kunnen momenteel ter analyse worden verzonden: (Alle releases

die File Analysis ondersteunen) Windows Executables, bijvoorbeeld .exe, .dll, .sys en .scr bestanden.Adobe Portable Document Format (PDF), Microsoft Office 2007+ (Open XML), Microsoft Office 97-2004 (OLE), Microsoft Windows/DOS Execteerbaar, andere potentieel kwaadaardige bestandstypen.Bestandstypen die u hebt geselecteerd voor het uploaden op de pagina anti-Malware en reparatie-instellingen (voor webbeveiliging) of de pagina Bestanden uploaden en analyseren (voor e-mail security). Initiële ondersteuning omvat PDF- en Microsoft Office-bestanden.(Beginnend in AsyncOS 9.7.1 voor e-mailbeveiliging) Als u de andere potentieel kwaadaardige bestandstypes hebt geselecteerd, dienen Microsoft Office-bestanden met de volgende uitbreidingen te worden opgeslagen in XML- of MHTML-indeling: ade, adp, en, accdb, accdr, accdr, accda, accda, mdb, cdb, mda, mdw, mdw, mdf, mdf, mde, accde, mam, maq, mar, mat, maf, ldb, laccdb, doc, dot, docx, dotx, dotm, docb, xls t, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xl, xlw, ppt, pot, pps, pptx, pptm, ptm, potx, ppam, ppsm, ppsm, sldx, sldm, mht, mhtm, html, en.

Opmerking: Als de lading in de dienst Bestandsanalyse de capaciteit overschrijdt, kunnen sommige bestanden niet worden geanalyseerd, zelfs als het bestandstype is geselecteerd voor analyse en het bestand anders voor analyse in aanmerking komt. U ontvangt een melding als de service bestanden van een bepaald type tijdelijk niet kan verwerken.

Belangrijke opmerkingen benadrukken:

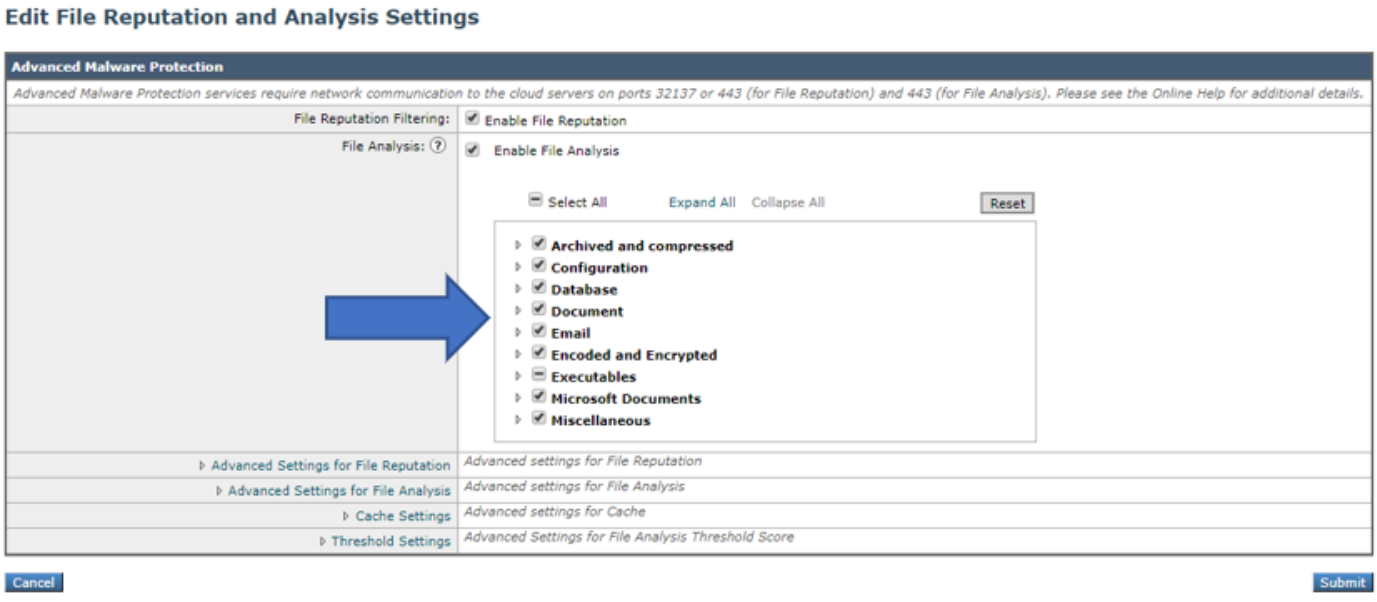
- Als er onlangs een bestand vanuit een bron is geüpload, wordt het bestand niet meer geüpload. Voor resultaten van bestandsanalyse voor dit bestand, zoek naar de SHA-256 op de rapportagepagina voor bestandsanalyse.
- Het apparaat probeert het bestand eenmaal te uploaden; als het uploaden niet geslaagd is, bijvoorbeeld vanwege aansluitingsproblemen, is het mogelijk dat het bestand niet wordt geüpload. Als de fout was opgetreden nadat de bestandsindeling was overbelast, wordt opnieuw geüpload.

AMP configureren voor bestandsanalyse

Wanneer een ESA voor het eerst wordt ingeschakeld en nog geen verbinding met het Cisco update-systeem moet maken, wordt standaard het ENLY File Analysis File type weergegeven door "Microsoft Windows/DOS Execteerbare" bestanden. U moet toestaan dat een servicetoepassing voltooid is voordat u toestemming krijgt om extra bestanden te configureren. Dit zal worden weerspiegeld in het logbestand update_logs, dat als "vuuramp.json" wordt gezien:

```
Sun Jul 9 13:52:28 2017 Info: amp beginning download of remote file
"http://updates.ironport.com/amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp successfully downloaded file
"amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp applying file "amp/1.0.11/fireamp.json/default/100116"
```

Om de bestandsindeling via de GUI te configureren **navigeer** naar **Beveiligingsservices > Bestandsrevaluatie en -analyse > Global Settings..**



Om AMP voor Bestandsanalyse te configureren via de CLI, voert u de **ampfig > Setup**-opdracht in en beweegt u door de wizard. U moet **Y** selecteren wanneer u deze vraag ontvangt: **Wilt u de bestandstypen voor File Analysis wijzigen?**

```
myesa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> setup

File Reputation: Enabled
Would you like to use File Reputation? [Y]>

Would you like to use File Analysis? [Y]>

File types supported for File Analysis:

1. Archived and compressed [selected]
2. Configuration [selected]
3. Database [selected]
4. Document [selected]
5. Email [selected]
6. Encoded and Encrypted [selected]
7. Executables [partly selected]
8. Microsoft Documents [selected]
9. Miscellaneous [selected]

Do you want to modify the file types selected for File Analysis? [N]> y
```

```
Enter comma separated serial numbers from the "Supported" list. Enter "ALL" to select all
"currently" supported File Types.
[1,2,3,4,5]> ALL

Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy.
```

Op basis van deze configuratie zijn de bestandstypen die ingeschakeld zijn onderworpen aan File Analysis, naar gelang het geval.

AMP-bestanden bekijken voor bestandsanalyse

Wanneer bijlagen zijn gescand met File Reputation of File Analysis op de ESA, worden ze opgenomen in het AMP-logbestand. Om dit logbestand te bekijken voor alle AMP-acties, **voert u** het **staart-indicatielampje** uit de CLI van de ESA, of gaat u door de antwoordwizard voor ofwel de **staart** of de **grep** opdracht. De **grep**-opdracht is handig als u het specifieke bestand kent of andere details wilt doorzoeken in het AMP-logbestand.

Hierna volgt een voorbeeld:

```
mylocal.esa >  tail amp

Press Ctrl-C to stop.
Tue Aug 13 17:28:47 2019 Info: Compressed/Archive File: sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac MID = 1683600, Extracted File: File Name =
'[redacted].pdf', File Type = 'application/pdf', sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac, Disposition = LOWRISK, Response received from =
Cloud, Malware = None, Analysis Score = 0, upload_action = Recommended to send the file for
analysis
Thu Aug 15 13:49:14 2019 Debug: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Thu Aug 15 13:49:14 2019 Debug: Response received for file reputation query from Cloud. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

> Opmerking: Oudere versies van AsyncOS zouden "amp_watchdog.txt" in de AMP-bestanden weergeven. Dit is een OS-bestand dat elke tien minuten in de loggen wordt weergegeven. Dit bestand maakt deel uit van de tijdens de opslag van AMP overgebleven informatie en kan veilig worden genegeerd. Dit bestand is verborgen vanaf AsyncOS 10.0.1 en nieuwer.

> Opmerking: Oudere versies van AsyncOS zullen het uploadaction tag registreren heeft drie waarden die zijn gedefinieerd voor het gedrag van het uploaden naar bestandsanalyse.

De drie reacties voor het uploaden van actie op oudere AsyncOS:

- "upload_action = 0": Het dossier is bekend bij de reputatieservice; niet ter analyse sturen.
- "upload_action = 1": Verzenden

- "upload_action = 2": Het dossier is bekend bij de reputatieservice; sturen niet naar analyse

De twee reacties voor uploadactie op AsyncOS versie 12.x en volgende:

- "upload_action = Aanbevolen om het bestand voor analyse te verzenden"
- **Alleen debug's:** "upload_action = Aanbevolen om het bestand voor analyse niet te verzenden"

Deze reactie dicteert of een bestand ter analyse wordt verzonden. Opnieuw moet het voldoen aan de criteria van de geconfigureerde bestandstypen om succesvol te kunnen worden ingediend.

Uitleg van de uploadactietekens

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`

Voor "0" betekent dit dat het bestand "niet hoeft te worden verzonden voor uploaden". Of, een betere manier om het te bekijken is, het bestand *kan indien* nodig voor het uploaden naar File Analysis worden verzonden. Als het bestand echter *niet* vereist is, wordt het bestand niet verzonden.

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`

Voor "2," is dit een strikte "stuur" het bestand niet om te uploaden. Deze actie is definitief en van doorslaggevend belang en de verwerking van bestandsanalyse wordt uitgevoerd.

Bijvoorbeeld scenario's

In dit gedeelte worden mogelijke scenario's beschreven waarin bestanden op de juiste manier worden geüpload of om een bepaalde reden niet worden geüpload.

Bestand uploaden voor analyse

Oudere AsyncOS:

Dit voorbeeld toont een DOCX-bestand dat voldoet aan de criteria en is gelabeld met de **upload_action = 1**. In de volgende regel **wordt** het **Bestand** dat **voor analyse** Secure Hash Algorithm (SHA) is geüpload ook geregistreerd op het AMP-logbestand.

```
Thu Jan 29 08:32:18 2015 Info: File reputation query initiating. File Name = 'Lab_Guide.docx',
MID = 860, File Size = 39136 bytes, File Type = application/msword
Thu Jan 29 08:32:19 2015 Info: Response received for file reputation query from Cloud. File Name
= 'Royale_Raman_Lab_Setup_Guide_Beta.docx', MID = 860, Disposition = file unknown, Malware =
None, Reputation Score = 0, sha256 =
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce, upload_action = 1
Thu Jan 29 08:32:21 2015 Info: File uploaded for analysis. SHA256:
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce
```

AsyncOS 12.x en verder:

Dit voorbeeld toont een PPTX-bestand dat aan de criteria voldoet en is gelabeld met de **upload_action = Aanbevolen om het bestand voor analyse te verzenden**. Op de volgende regel **wordt** het **bestand dat voor analyse** Secure Hash Algorithm (SHA) is **geüpload** ook opgenomen in het AMP-logbestand.

```
Thu Aug 15 09:42:19 2019 Info: Response received for file reputation query from Cloud. File Name
= 'ESA_AMP.pptx', MID = 1763042, Disposition = UNSCANNABLE, Malware = None, Analysis Score = 0,
sha256 = 0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, upload_action = Recommended to
send the file for analysis
Thu Aug 15 10:05:35 2019 Info: File uploaded for analysis. SHA256:
0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, file name: ESA_AMP.pptx
```

Bestand niet geüpload voor analyse omdat bestand al bekend is

Oudere AsyncOS:

Dit voorbeeld toont een PDF-bestand dat door AMP is gescand met de **upload_action = 2** toegevoegd aan het bestand reputatielog. Dit bestand is al bekend bij de Cloud en hoeft niet te worden geüpload voor analyse, zodat het niet meer wordt geüpload.

```
Wed Jan 28 09:09:51 2015 Info: File reputation query initiating. File Name = 'Zombies.pdf', MID
= 856, File Size = 309500 bytes, File Type = application/pdf
Wed Jan 28 09:09:51 2015 Info: Response received for file reputation query from Cache. File Name
= 'Zombies.pdf', MID = 856, Disposition = malicious, Malware = W32.Zombies.NotAVirus, Reputation
Score = 7, sha256 = 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002,
upload_action = 2
```

AsyncOS 12.x en verder:

Dit voorbeeld toont het amp_watchdog.txt-bestand met IP-logbestanden op debug-niveau die overeenkomen met het **uploadactie = Aanbevolen om het bestand niet te verzenden voor analyse** die is toegevoegd aan het bestand dat **wordt** reputatie heeft. Dit bestand is al bekend bij de Cloud en hoeft niet te worden geüpload voor analyse, zodat het niet meer wordt geüpload.

```
Mon Jul 15 17:41:53 2019 Debug: Response received for file reputation query from Cache. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

Loging File Analysis Upload via e-mailheaders

Vanaf de CLI, met de optie die de opdracht **logfig** gebruikt, kan de suboptie van **logheaders** worden geselecteerd om de kopregels van e-mails die via het ESA zijn verwerkt op te geven en te registreren. Met de "X-Amp-File-Upload" header wordt altijd een bestand geüpload of niet geüpload voor bestandsanalyse opgenomen in de postbestanden van het ESA.

Wanneer u de e-mailbestanden bekijkt, zijn de resultaten voor de bestanden die voor analyse zijn geüpload:

```
Mon Sep 5 13:30:03 2016 Info: Message done DCID 0 MID 7659 to RID [0] [('X-Amp-File-Uploaded',
'True')]
```

Wanneer u de e-mailbestanden bekijkt, zijn de resultaten voor bestanden die niet voor analyse zijn geüpload:

```
Mon Sep 5 13:31:13 2016 Info: Message done DCID 0 MID 7660 to RID [0] [('X-Amp-File-Uploaded',
'False')]
```

Gerelateerde informatie

- Async-gebruikershandleidingen
- Bestandscriteria voor geavanceerde Malware Protection Services voor Cisco Content Security Producten
- ESA Advanced Malware Protection (AMP) Test
- Technische ondersteuning en documentatie – Cisco Systems