Konfigurieren des Scanners für Bedrohungen pro Richtlinie für SEG

Inhalt

Einleitung

In diesem Dokument werden der Service und die Konfiguration von Threat Scanner (TS) Per Policy Integration für das Cisco Secure Email Gateway (SEG) beschrieben.

Voraussetzungen

Kenntnis der allgemeinen SEG-Einstellungen und -Konfiguration ist erwünscht.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 und höher
- Graymail-Dienst.
- Antispam-Dienst.
- Richtlinien für eingehende Mails.

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.

Überblick

Threat Scanner (TS), eine neu aktivierte Unterkomponente des Graymail-Dienstes, wurde in Antispam CASE integriert, um eine effektivere AntiSpam-Erkennung zu ermöglichen.

Sobald der Graymail-Dienst aktiviert wurde, werden die Optionen zur Aktivierung des Bedrohungsscanners innerhalb jeder AntiSpam-Einstellung der Mail-Policy für eingehende Nachrichten aktiviert. Sobald TS aktiviert ist, verbessert sich die Antispam-Erkennung mit Schwerpunkt auf der HTML-Schmuggelerkennung:

- HTML-Analyse und Erkennung schädlicher Skripts
- Erkennung von URL-Parsing und -Umleitung

Die Antispam CASE Engine regelt die beiden Dienste, verwaltet Updates und Spam-Verurteilungen.

TS verfügt über sichtbare Aktivierungs-/Deaktivierungseinstellungen innerhalb jeder Antispam-Einstellung für eingehende E-Mails.

TS beeinflusst Urteile und erhöht das Gewicht des endgültigen Antispam-Urteils.

Konfigurieren

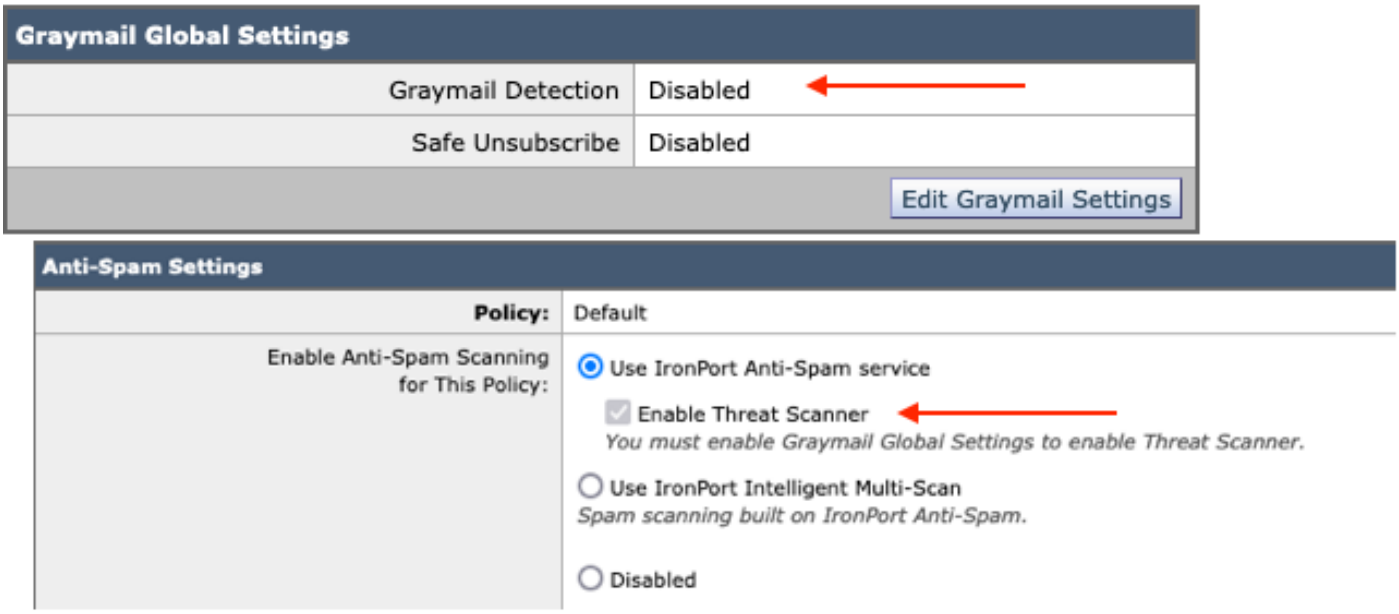
Die Konfiguration besteht aus zwei Aktionen: "Graymail-Erkennung aktivieren" und "TS innerhalb der Posteingangsrichtlinien aktivieren".

- Der globale Graymail-Dienst muss aktiviert sein, um TS zu aktivieren.
- Sobald Graymail global aktiviert ist, wird die Option "Anti-Spam" der Inbound Mail Policy auf "Enable Threat Scanner" aktiviert.

Einrichtung der Webschnittstelle

So aktivieren Sie Graymail in der WebUII:

- Zu Sicherheitsservices navigieren
    - IMS und Graymail
        - Globale Graymail-Einstellungen
            - Graymail-Einstellungen bearbeiten.
                - Wählen Sie die Option aus, um die Graymail-Erkennung zu aktivieren.
- Senden und bestätigen Sie die Änderungen, um die Aktion abzuschließen.

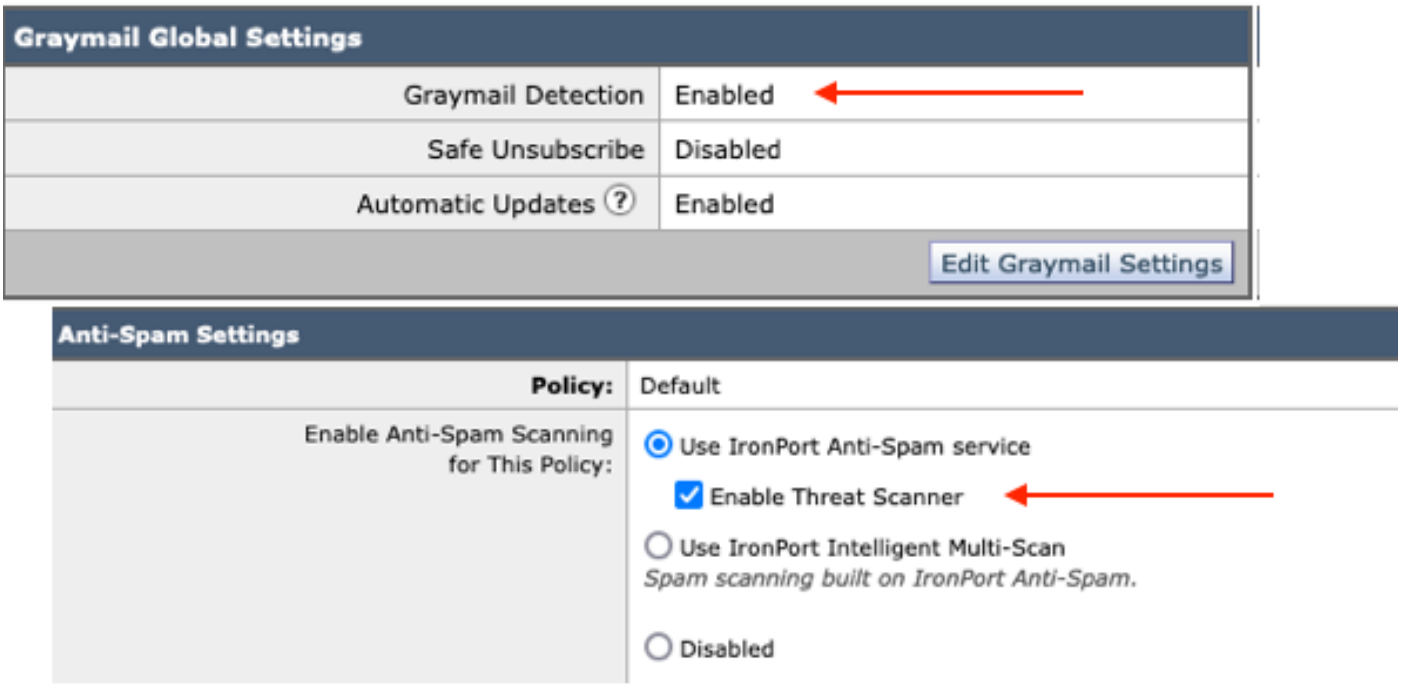


Die Ansicht vor der Einrichtung

Sobald Graymail aktiviert wurde, wird das Auswahlfeld Bedrohungsscanner für jede Richtlinie für eingehende E-Mails verfügbar.

So aktivieren Sie Threat Scanner in der WebUI:

- Navigieren zu Mail-Policys
  - Richtlinien für eingehende Mails
    - Wählen Sie die gewünschte E-Mail-Richtlinie aus
      - Wählen Sie Anti-Spam aus.
        - Oben auf der Konfigurationsseite wird das Kontrollkästchen Enable Threat Scanner (Bedrohungsscanner aktivieren) angezeigt.
- Senden und bestätigen Sie die Änderungen, um die Konfiguration abzuschließen.



Die Threat Scanner-Option in Antispam

Einrichtung der Befehlszeilenschnittstelle

Aktivieren Sie den Graymail-Dienst mithilfe der CLI-Befehle.

- imsandgraymailconfig
    - Gymail
        - Einrichtung
            - Möchten Sie Graymail Detection verwenden? [J] >
                - Möchten Sie automatische Updates für die Graymail-Engine aktivieren? [J]>
    - Beenden Sie die verbleibenden Aufforderungen, um zur Eingabeaufforderung des Hauptcomputers zurückzukehren.

- Bestätigen + gewünschte Kommentare hinzufügen > Beenden Sie die Aktion, indem Sie die Eingabetaste drücken.

Aktivieren oder Deaktivieren des Bedrohungsscanners innerhalb einer Richtlinie über die CLI.

- CLI> Richtlinienkonfiguration

Möchten Sie Richtlinien für eingehende E-Mails oder Richtlinien für ausgehende E-Mails konfigurieren oder die Header-Priorität zuordnen?

1. Richtlinien für eingehende Mails
2. Richtlinien für ausgehende Mails
3. Header-Priorität zuordnen

[1]> 1

Konfiguration der eingehenden Mail-Policy

1. Nord1
2. GESPERRTE LISTE
3. ZULÄSSIGE_LISTE
4. ALLOW_SPOOF
5. STANDARD

Geben Sie den Namen oder die Nummer des Eintrags ein, den Sie bearbeiten möchten:
[]> 1

Wählen Sie den Vorgang aus, den Sie ausführen möchten:
- NAME - Ändern des Namens der Richtlinie
- NEU - Fügt eine neue Policy-Member-Zeile hinzu
- DELETE - Entfernt eine Policy-Mitgliedszeile
- PRINT - Drucken von Mitgliederzeilen der Richtlinie
- ANTISPAM - Anti-Spam-Richtlinie ändern
- ANTIVIRUS - Anti-Virus-Richtlinie ändern
- OUTBREAK - Outbreak-Filterrichtlinie ändern

- ADVANCEDMALWARE - Advanced Malware Protection-Richtlinie ändern
- GRAYMAIL - Ändern der Graymail-Richtlinie
- THREATDEFENSECONNECTOR - Ändern des Anschlusses für die Bedrohungsabwehr
- FILTER - Filter ändern
[]> Antispam

Wählen Sie den Vorgang aus, den Sie ausführen möchten:
- DISABLE - Anti-Spam-Richtlinie deaktivieren (Deaktiviert alle richtlinienbezogenen Aktionen)
- ENABLE - Anti-Spam-Richtlinie aktivieren
[]> Aktivieren

Anti-Spam-Konfiguration starten

Möchten Sie Intelligentes Mehrfach-Scannen für diese Richtlinie verwenden? [N]>

Möchten Sie IronPort Anti-Spam für diese Richtlinie verwenden? [J]>

Einige Nachrichten werden positiv als Spam identifiziert. Einige Nachrichten sind
als Spam-verdächtig identifiziert. Sie können den IronPort Anti-Spam Suspected Spam
Schwellenwert unter.
Die Konfigurationsoptionen gelten für Nachrichten, die POSITIV als
Spam:
Möchten Sie die Sonderbehandlung für das Verdict von Threat Scanner aktivieren? [N]> J

Fahren Sie mit der Auswahl im Menü fort, um die Mail Policy-Auswahl abzuschließen, und drücken Sie die "Return"-Taste, um die Standardaktion für jede Auswahl zu akzeptieren.

Schließen Sie das Speichern mit den Befehlen ab.

- Bestätigen + gewünschte Kommentare hinzufügen > Beenden Sie die Aktion, indem Sie die Eingabetaste drücken.

Überprüfung

Lesen und Interpretieren der Protokolle

Mail Logging of Threat Scanner stellt lediglich ein Zwischenurteil dar, während CASE das endgültige Urteil präsentiert.

Die E-Mail-Protokolle enthalten zwei verschiedene Verdicts für unschädliche und für schuldig befundene Threat Scanner-Verdicts.

- Wenn das Interim-Urteil des Threat Scanners unschädlich ist, wird das Protokoll ähnlich wie in diesen Beispielen angezeigt.
    - Info: Interim Graue Nachricht - LEGIT (0) <Saubere Nachricht>
    - Info: Interim Graustufenurteil - MCE (11) <Verschiedene E-Mail-Kampagnen>
- Wenn das Threat Scanner-Interim-Urteil rechtskräftig wird, wird das Protokoll ähnlich wie bei

diesen Stichproben angezeigt.
- Info: Interim ThreatScanner-Urteil - PHISHING (101)
- Info: Zwischenurteil von ThreatScanner - VIRUS (2)

Mail-Protokolle Beispiel: Threat Scanner Clean Verdict verwendet verschiedene Verdict: Graymail Verdict.

<#root>

```
Wed Jan 31 08:19:32 2024 Info: MID 3189755
```

interim graymail verdict - LEGIT (0) <Clean message>

```
Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative
Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative
```

Bei der Nachrichtenverfolgung wird der Eintrag im Threat Scanner-Protokoll nicht angezeigt, sondern nur der CASE: Final Verdict.

Diese Beispiele von Threat Scanner (TS) stellen die 4 Verdict-Szenarien dar.

Hinweis: Die TS-Kategorien "PHISHING" und "VIRUS" sind die einzigen Erkennungsmerkmale, die das Gewicht des FALLURTEILS erhöhen.

Beispiel für Mail-Protokolle: PHISHING TS Conviction und AntiSpam Conviction sind beide vorhanden

<#root>

```
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

interim

ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

using engine: CASE spam positive

```
Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE
```

Tracking-Beispiel: PHISHING TS-Verurteilung fehlt und CASE-Verurteilung ist vorhanden.

25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive

PHISHING TS verurteilt und Anti-Spam verurteilt Tracking

Mail Logs Sample: PHISHING TS Conviction und AntiSpam Negative sind beide vorhanden.

<#root>

```
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

interim ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

using engine: CASE spam negative

Tracking-Beispiel: PHISHING TS Convicted und AntiSpam Negative ist vorhanden.

25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative

Mail-Protokolle Beispiel: VIRUS TS Conviction und AntiSpam Conviction Beispiel der Mail-Protokolle.

<#root>

```
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim
```

ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive
Thu Jan 25 13:37:16 2024 Info: MID 3066060
```

using engine: CASE spam positive

```
Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE
```

Beispiel für die Nachverfolgung: VIRUS TS-Verurteilung abwesend und AntiSpam-Verurteilung vorhanden.

25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 aborted: Dropped by CASE

Beispiel für Mail-Protokolle: VIRUS TS Conviction und AntiSpam Negative sind beide vorhanden.

<#root>

```
Jan 23 21:38:57 2024 Info: MID 3013692
```

interim ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative
Jan 23 21:38:58 2024 Info: MID 3013692
```

using engine: CASE spam negative

Tracking-Beispiel: VIRUS TS-Verurteilung abwesend und AntiSpam Negative vorhanden.

23 Jan 2024 19:38:57 (GMT -08:00)	Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative

Graymail Logs enthalten das Urteil des Threat Scanners und unterstützende Inhalte für die TALOS-Analyse, wenn eine falsch-positive Herausforderung gemacht wird.

Das Vorhandensein der Ergebnisse des Threat Scanners führte zu einem schnelleren Rollover der Graymail-Protokollierung. Um diesem Verhalten entgegenzuwirken, wurden die SEG-Änderungen an den Graymail-Protokollen vorgenommen.

- AsyncOS 15.5 setzt die Standard-Protokoll-Subscription für Graymail-Protokolldateien auf 20, um die Protokollaufbewahrung zu verbessern.
  - Die Einstellungen für die Protokolldatei ändern sich nicht, wenn beim Upgrade eine Einstellung von mehr als 20 festgelegt wird.
- Eingehende Graymail Interim überführte Nachrichten zeigen volle Scan-Roh-Ergebnisse, auf der Informationsebene.
- Die Ergebnisse der Graymail-Suche für alle anderen Nachrichten werden auf der Debugstufe angezeigt.

Zugehörige Informationen

- Email Security - Einrichtungsleitfaden
- Cisco Secure Email Gateway Launch-Website für Support-Leitfäden

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.