Configurazione dell'analisi per criterio di Threat Scanner per SEG

Sommario

Introduzione

Questo documento descrive il servizio e la configurazione di Threat Scanner (TS) per l'integrazione dei criteri per Cisco Secure Email Gateway (SEG).

Prerequisiti

È necessario conoscere le impostazioni generali e la configurazione di SEG.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e versioni successive.
- Servizio Graymail.
- Servizio Antispam.
- Criteri posta in arrivo.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Threat Scanner (TS), un nuovo sottocomponente attivato del servizio Graymail, è stato integrato con Antispam CASE per fornire un rilevamento più efficace di AntiSpam.

Dopo l'attivazione del servizio Graymail, le opzioni per l'abilitazione di Threat Scanner diventano attive all'interno di ciascuna impostazione AntiSpam dei criteri della posta in arrivo. Una volta abilitato TS, migliora il rilevamento Antispam complessivo con un'enfasi sul rilevamento di contrabbando HTML:

- Analisi HTML e rilevamento di script dannosi
- Rilevamento analisi e reindirizzamento URL

Il motore Antispam CASE gestisce i due servizi, gestendo gli aggiornamenti e le condanne per spam.

In Servizi terminal sono disponibili impostazioni di attivazione/disattivazione visibili all'interno di ogni impostazione Antispam dei criteri della posta in arrivo.

TS influenza i verdetti, aumentando il peso del verdetto finale del CASO Antispam.

Configurazione

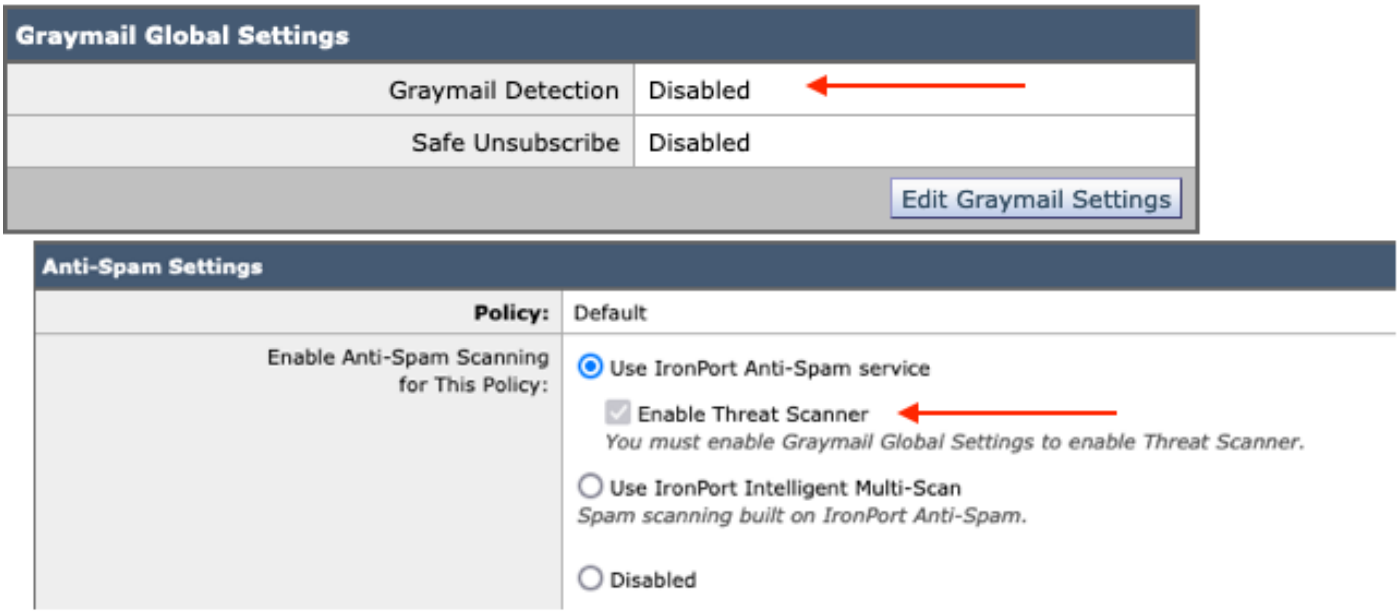
La configurazione è costituita da due azioni: Abilita rilevamento posta grigia e Abilitazione di Servizi terminal nei criteri di posta in arrivo.

- Per attivare Servizi terminal, è necessario che il servizio globale Graymail sia abilitato.
- L'opzione "Antispam" del criterio della posta in arrivo per "Abilita scanner minacce" diventa disponibile dopo che Graymail è stato abilitato a livello globale.

Installazione interfaccia Web

Per abilitare Graymail all'interno di WebUII:

- Passa a Servizi di sicurezza
    - IMS e Graymail
        - Impostazioni globali posta grigia
            - Modifica impostazioni posta grigia.
                - Selezionare l'opzione per abilitare il rilevamento della posta grigia.
- Sottomettere e confermare le modifiche per finalizzare l'azione.

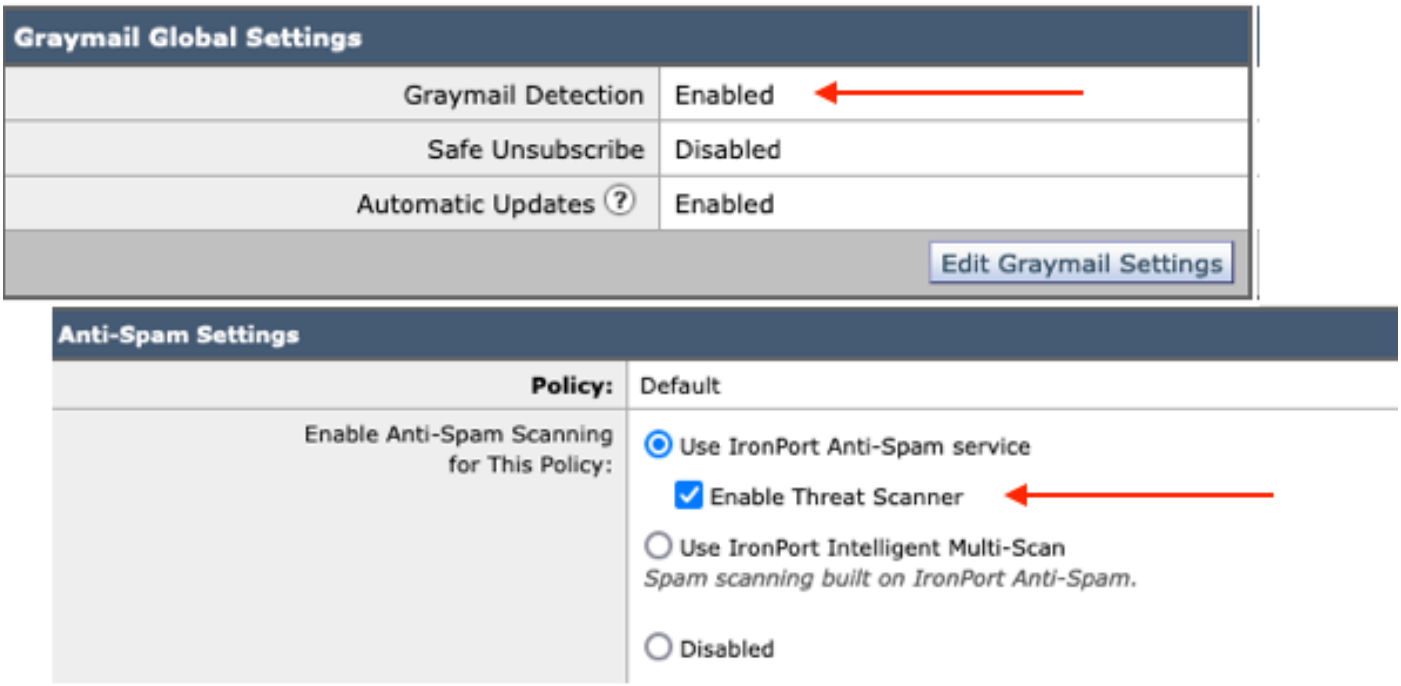


Visualizzazione prima dell'installazione

Dopo aver abilitato Graymail, la casella di selezione Scanner minaccia diventa disponibile per ogni Criterio posta in arrivo.

Per abilitare Threat Scanner all'interno di WebUI:

- Passa a Criteri di posta
  - Criteri posta in arrivo
    - Selezionare il criterio di posta desiderato
      - Selezionare Anti-Spam.
        - Nella parte superiore della pagina di configurazione è presente l'opzione della casella di controllo Abilita Threat Scanner.
- Inviare e confermare le modifiche per finalizzare la configurazione



Opzione Threat Scanner in Antispam

Installazione dell'interfaccia della riga di comando

Abilitare il servizio Greymail usando i comandi CLI.

- imsandgraymailconfig
  - posta grigia
    - configurazione
      - Utilizzare il rilevamento della posta grigia? [S] >
        - Abilitare gli aggiornamenti automatici per il motore Graymail? [S]>
  - Completate i prompt rimanenti per tornare al prompt della macchina principale.

- Conferma + aggiungi i commenti desiderati > Completa l'azione premendo il tasto "Invio".

Abilitazione o disabilitazione di Threat Scanner all'interno di una policy dalla CLI.

- CLI> policyconfig

Configurare i criteri di posta in arrivo o in uscita oppure la priorità di corrispondenza delle intestazioni?

1. Criteri posta in arrivo
2. Criteri posta in uscita
3. Associa priorità intestazioni

[1]> 1

Configurazione criteri posta in arrivo

1. Nord 1
2. ELENCO_BLOCCATO
3. ELENCO_CONSENTITO
4. ALLOW_SPOOF
5. VALORE PREDEFINITO

Immettere il nome o il numero della voce da modificare:
[]> 1

Scegliere l'operazione da eseguire:
- NAME - Modifica il nome del criterio
- NUOVO - Aggiungi una nuova riga di membro del criterio
- DELETE - Rimuove la riga di un membro del criterio
- PRINT - Stampa le righe dei membri del criterio
- ANTISPAM - Modifica criteri antispam
- ANTIVIRUS - Modifica criteri antivirus
- EPIDEMIE - Modifica il criterio dei filtri epidemie
- ADVANCEDMALWARE - Modifica criteri di protezione avanzata da malware
- GRAYMAIL - Modifica criterio Graymail
- THREATDEFENSECONNECTOR - Modifica connettore di difesa dalle minacce

- FILTRI - Modifica filtri
[]> antispam

Scegliere l'operazione da eseguire:
- DISABLE - Disabilita i criteri antispam (disabilita tutte le azioni correlate ai criteri)
- ENABLE - Abilita criteri antispam
[]> abilita

Inizio configurazione posta indesiderata

Utilizzare Multi-Scan intelligente per questo criterio? [N]>

Utilizzare IronPort Anti-Spam in questo criterio? [S]>

Alcuni messaggi vengono identificati come posta indesiderata. Alcuni messaggi sono identificate come sospette spam. È possibile impostare IronPort Anti-Spam Suspected Spam Soglia inferiore.
Le opzioni di configurazione si applicano ai messaggi identificati positivamente come posta indesiderata:
Si desidera abilitare un trattamento speciale per il verdetto dello scanner di minaccia? [N]> s

Continuare con le selezioni di menu per completare le scelte dei criteri di posta e premere il tasto Invio per accettare l'azione predefinita per ogni scelta.

Completare il salvataggio con i comandi.

- Conferma + aggiungi i commenti desiderati > Completa l'azione premendo il tasto "Invio".

Verifica

Come leggere e interpretare i registri.

La registrazione della posta di Threat Scanner emette solo un verdetto provvisorio, mentre CASE emette il verdetto finale.

I log di posta mostrano due verbi diversi per i verdetti puliti rispetto ai verdetti condannati dello scanner di minaccia

- Se il verdetto provvisorio dello scanner di minaccia è pulito, il registro viene presentato in modo simile a questi esempi.
  - Info: verdetto provvisorio in grigi - LEGIT (0) <Messaggio pulito>
  - Info: verdetto provvisorio griymail - MCE (11) <Campagna e-mail varie>
- Se il verdetto provvisorio dello scanner di minaccia deve essere condannato, il registro viene presentato in modo simile a questi campioni.
  - Info: interim ThreatScanner verdict - PHISHING (101)
  - Informazioni: verdetto provvisorio ThreatScanner - VIRUS (2)

Esempio di log di posta: Threat Scanner Clean verdict utilizza un verbiage diverso: verdict di

graymail.

<#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
```

Message Tracking non visualizza la voce del log dello scanner di minacce, ma solo il caso: verdetto finale.

Questi esempi di Threat Scanner (TS) presentano i 4 scenari del verdetto.

Nota: le categorie TS di "PHISHING" e "VIRUS" sono le uniche rilevazioni che aumentano la rilevanza del caso

---

Esempio di log di posta: sono presenti sia la condanna di Servizi terminal di PHISHING che la condanna antispam

<#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
```

Esempio di rilevamento: la condanna TS per il PHISHING è assente ed è presente la condanna CASE.

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

Monitoraggio dei servizi terminal di PHISHING condannati e AntiSpam condannati

Esempio di log di posta: sono presenti sia la condanna TS per il PHISHING che la posta indesiderata negativa.

<#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

Esempio di rilevamento: TS di PHISHING condannato e AntiSpam negativo presente.

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

Esempio di log di posta: esempio di virus TS Conviction e AntiSpam Conviction dei log di posta.

<#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
```

Esempio di rilevamento: assenza di condanna TS per il virus e condanna antispam presente.

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

Esempio di log di posta: sono presenti sia virus TS Conviction che AntiSpam Negative.

<#root>

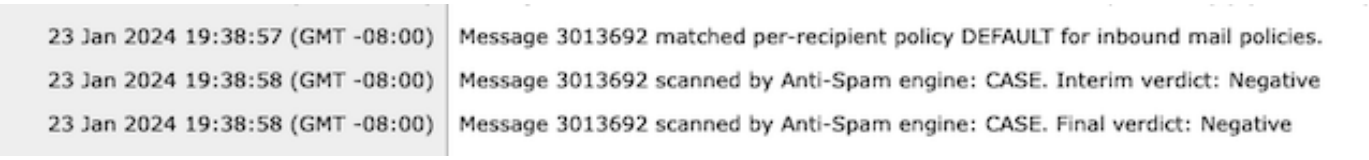
```
Jan 23 21:38:57 2024 Info: MID 3013692

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
```

Esempio di rilevamento: sospetto TS per il virus assente e negativo per antispam presente.



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

I log di Graymail contengono il verdetto Threat Scanner e il contenuto di supporto per l'analisi TALOS se viene fatta una falsa sfida positiva.

La presenza dei risultati non elaborati di Threat Scanner ha causato il rollover più rapido della registrazione di Graymail. Per risolvere questo problema, sono state apportate modifiche SEG ai log di Graymail.

- AsyncOS 15.5 imposta su 20 la sottoscrizione di log predefinita per i file di log di Graymail per una maggiore conservazione dei log.
  - Le impostazioni del file di registro non vengono modificate se al momento dell'aggiornamento l'impostazione è superiore a 20.
- I messaggi in ingresso con stato Condanna Interim Graymail visualizzano i risultati non elaborati dell'analisi completa, a livello di informazioni.
- I risultati dell'analisi da parte di Graymail per tutti gli altri messaggi vengono visualizzati a livello di debug.

Informazioni correlate

- Guida alla configurazione di Email Security
- Pagina di avvio di Cisco Secure Email Gateway per il supporto delle guide

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).