

# Scanner per-beleid voor SEG configureren

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Configureren](#)

[Web interface instellen](#)

[Instellen interface opdrachtregel](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft de service en configuratie van Threat Scanner (SEG) per beleidsintegratie voor Cisco Secure Email Gateway (SEG).

## Voorwaarden

Kennis van de algemene instellingen en configuratie van de SEG is gewenst.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 en nieuwer.
- Graymail-service.
- Antispam-service.
- Inkomende post beleid.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Overzicht

Threat Scanner (TS), een nieuw geactiveerd onderdeel van de Graymail-service, is geïntegreerd met Antispam CASE waardoor de detectie van antiSpam effectiever is.

Nadat de Graymail-service is geactiveerd, worden opties om Threat Scanner in te schakelen actief binnen elke instelling voor Inkomende Mail Policy AntiSpam. Eenmaal ingeschakeld TS verbetert

de algemene antispam-detectie met een nadruk op HTML-smokkel detectie:

- HTML-parsing en kwaadaardige scriptdetectie
- URL-parsing en detectie van omleiding

De Antispam CASE engine regelt de twee diensten, het beheren van updates en spam veroordelingen.

TS heeft zichtbare in-/uitschakelen instellingen binnen elke Inkomende Mail Policy Antispam-instelling.

TS beïnvloedt vonnissen, waardoor het gewicht van de uiteindelijke Antispam CASE vonnis.

## Configureren


Configuratie bestaat uit twee acties: Schakel de optie Graymail-detectie in en schakel de optie TS in binnen het beleid voor inkomende e-mail.

- De wereldwijde dienst van Graymail moet worden toegelaten om TS te activeren.
- De optie "Antispam" van Inbound Mail Beleid om "Threat Scanner inschakelen" wordt beschikbaar zodra Graymail wereldwijd is ingeschakeld.


## Web interface instellen

U kunt als volgt Graymail inschakelen in de WebUI:

- Naar beveiligingsservices navigeren
  - IMS en Graymail
    - Wereldwijde Graymail-instellingen
      - Grijsmail-instellingen bewerken.
        - Selecteer de optie om Graymail Detectie in te schakelen.
- Verzend de wijzigingen en leg ze vast om de actie te voltooien.

Graymail Global Settings	
Graymail Detection	Disabled 
Safe Unsubscribe	Disabled

[Edit Graymail Settings](#)

Anti-Spam Settings	
<b>Policy:</b>	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Enable Threat Scanner  <i>You must enable Graymail Global Settings to enable Threat Scanner.</i></li><li><input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i></li><li><input type="radio"/> Disabled</li></ul>

Zodra Graymail is ingeschakeld, wordt het selectievakje Threat Scanner beschikbaar voor elk inkomend mailbeleid.

U kunt Threat Scanner als volgt inschakelen binnen de Webex UI:

- Naar mailbeleid navigeren
  - Beleid voor inkomende e-mail
    - Selecteer het gewenste mailbeleid
      - Selecteer anti-spam.
        - Bovenaan de configuratiepagina staat de optie van het aankruisvakje om Threat Scanner in te schakelen.
- Verzend de wijzigingen en leg ze vast om de configuratie te voltooien

Graymail Global Settings	
Graymail Detection	Enabled ←
Safe Unsubscribe	Disabled
Automatic Updates (?)	Enabled

[Edit Graymail Settings](#)

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="checkbox"/> Enable Threat Scanner ← <input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

Optie Threat Scanner in Antispam

## Instellen interface opdrachtregel

Schakel de Graymail-service in met de CLI-opdrachten.

- `imsandgraymailconfig`
  - `grijsbrief`
    - `opstelling`
      - `Wilt u gebruik maken van Graymail Detection? [Y] >`
        - `Wilt u automatische updates voor Graymail engine inschakelen? [Y]>`
  - Voltooi de overige aanwijzingen om naar de hoofdprompt van het apparaat terug te keren.
- `Commit +` voeg gewenste opmerkingen toe `>` Voltooi de actie door op de "Return"-toets te drukken.

Threat Scanner in- of uitschakelen binnen een beleid van de CLI.

- CLI> Beleidsconfiguratie

Wilt u het beleid voor inkomende e-mail of het beleid voor uitgaande e-mail configureren of de prioriteit voor kopregels aanpassen?

1. Beleid voor inkomende e-mail
2. Beleid voor uitgaande post
3. Prioriteit matching-koppen

[1]> 1

Configuratie van inkomend mailbeleid

1. Noord1
2. GEBLOKKEERDE\_LIJST
3. TOEGESTAAN\_LIJST
4. ENABLE\_SPOOF
5. STANDAARD

Voer de naam of het nummer in van het item dat u wilt bewerken:

[]> 1

Kies de bewerking die u wilt uitvoeren:

- NAAM - Naam van beleid wijzigen
- NIEUW - Een nieuwe beleidsledenrij toevoegen
- VERWIJDEREN - Een regel verwijderen
- AFDRUKKEN - Ledenrijen afdrukken
- ANTISPAM - Antispambeleid wijzigen
- ANTIVIRUS - Antivirusbeleid wijzigen
- UITBRAAK - Aanpassen van uitbraakfilters beleid
- ADVANCED MALWARE - Wijzig het beleid voor Advanced Malware Protection
- GRAYMAIL - wijzigen Graymail beleid
- THREATDEFENSECONNECTOR - Threat Defence Connector wijzigen
- FILTERS - Filters wijzigen

[]> antispam

Kies de bewerking die u wilt uitvoeren:

- UITSCHAKELEN - anti-spambeleid uitschakelen (Schakelt alle beleidsgerelateerde acties uit)
- INSCHAKELEN - anti-spambeleid inschakelen

[]> inschakelen

Configuratie anti-spam starten

Wilt u Intelligent Multi-Scan gebruiken op dit beleid? [N]>

Wilt u IronPort Anti-Spam gebruiken voor dit beleid? [Y]>

Sommige berichten worden positief geïdentificeerd als spam. Sommige berichten zijn waarvan wordt vermoed dat het spam-virus aanwezig is. U kunt de instelling IronPort Anti-Spam Suspected Spam gebruiken

Drempel hieronder.

De configuratieopties zijn van toepassing op berichten DIE POSITIEF zijn geïdentificeerd als spam:

Wilt u een speciale behandeling voor het vonnis van Threat Scanner inschakelen? [N]> y

Ga verder door de menu-selecties om de Mail Policy keuzes te voltooien en druk op de "return key" om de standaard actie voor elke keuze te accepteren.

Vul het opslagproces in met de opdrachten.

- Commit + voeg gewenste opmerkingen toe > Voltooi de actie door op de "Return"-toets te drukken.

## Verifiëren

Hoe de logboeken te lezen en te interpreteren.

Mail Logging van Threat Scanner levert slechts een voorlopig vonnis, terwijl CASE het definitieve vonnis presenteert.

De mail logboeken tonen twee verschillende werkwoorden voor schone vs veroordeelde Threat Scanner vonnissen

- Als het vonnis van de Threat Scanner Interim schoon is, wordt het logboek op dezelfde manier getoond als deze steekproeven.
  - Info: tussentijds grijsbericht vonnis - LEGIT (0) <Bericht schoonmaken>
  - Info: tussentijds vonnis in grijsbrieven - MCE (11) <Diverse e-mailcampagne>
- Als het vonnis van de Threat Scanner Interim moet worden veroordeeld, wordt het logboek op dezelfde manier getoond als deze steekproeven.
  - Info: tussentijds vonnis ThreatScanner - PHISHING (101)
  - Info: tussenvonnis ThreatScanner - VIRUS (2)

Mail Logs Voorbeeld: Threat Scanner Clean verdict gebruikt verschillende woorden: graymail vonnis.

<#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

Berichttracering toont niet de logboek invoer van de Threat Scanner, alleen de CASE: Definitief vonnis.

Deze voorbeelden van Threat Scanner (TS) presenteren de 4 verdict scenario's.

---

 Opmerking: TS-categorieën van "PHISHING" en "VIRUS" zijn de enige detectie die het gewicht van de CASE Verdict verhogen

---

Mail Logs Voorbeeld: PHISHING TS Conviction en AntiSpam Conviction zijn beide aanwezig

<#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

Trackmonster: PHISHING TS-veroordeling is afwezig en de zaak is veroordeeld.

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

Veroordeelde PHISHING TS en antiSpam Veroordeelde Volgen

Mail Logs Sample: PHISHING TS Conviction en AntiSpam Negative zijn beide aanwezig.

<#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

Volgmonster: PHISHING TS Veroordeeld en AntiSpam Negatief is aanwezig.

```
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 Logs Monster: VIRUSSEN TS Conviction en AntiSpam Conviction sample van de mail logs.

<#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

Trackmonster: Virus TS veroordeling ontbreekt en AntiSpam veroordeling is aanwezig.

```
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
```

Mail Logs Voorbeeld: Virus TS Conviction en AntiSpam Negative zijn beide aanwezig.

<#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**

Trackmonster: Virus TS veroordeling ontbreekt en AntiSpam Negatief is aanwezig.

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 bevatten Threat Scanner uitspraak en ondersteunende inhoud voor TALOS analyse als een valse positieve uitdaging wordt gemaakt.

De aanwezigheid van de onbewerkte resultaten van de Threat Scanner heeft ervoor gezorgd dat de Graymail-logboekregistratie sneller kon worden omgedraaid. Om dit gedrag aan te pakken zijn de SEG wijzigingen aangebracht aan de Graymail Logs.

- AsyncOS 15.5 stelt het Default Log Subscription voor Graymail-logbestanden in op 20 voor een verhoogd logbehoud.
  - Geen wijzigingen in logbestanden als de instelling na de upgrade hoger dan 20 is ingesteld.
- Inkomende Graymail Interim veroordeelde berichten tonen volledige scan ruwe resultaten, op het informatieniveau.
- Grijsmail scanresultaten voor alle andere berichten weergeven op Debug niveau.

## Gerelateerde informatie

- [E-mail security installatiehandleiding](#)
- [Cisco Secure Email Gateway-startpagina voor ondersteuningshandleidingen](#)



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.