Configurar varredura por política do Threat Scanner para SEG

Contents

Introdução

Este documento descreve o serviço e a configuração do Threat Scanner (TS) por integração de política para o Cisco Secure Email Gateway (SEG).

Pré-requisitos

É desejável o conhecimento das configurações gerais do SEG.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e mais recente.
- Serviço Graymail.
- Antispam Service (Serviço antispam).
- Políticas de recebimento de e-mail.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

O Threat Scanner (TS), um subcomponente recém-ativado do serviço Graymail, foi integrado ao Antispam CASE, proporcionando uma detecção antisspam mais eficaz.

Depois que o serviço Graymail for ativado, as opções para ativar o Threat Scanner ficarão ativas em cada configuração de AntiSpam da política de e-mails recebidos. Uma vez habilitado, o TS melhora a detecção geral de antispam com ênfase na detecção de contrabando de HTML:

- Análise HTML e detecção de scripts mal-intencionados
- Análise de URL e detecção de redirecionamento

O mecanismo de caso antispam controla os dois serviços, gerenciando atualizações e condenações de spam.

O TS tem configurações visíveis para habilitar/desabilitar em cada configuração Antispam de Política de Email de Entrada.

O TS influencia os veredictos, aumentando o peso do veredito final do CASO Antispam.

Configurar

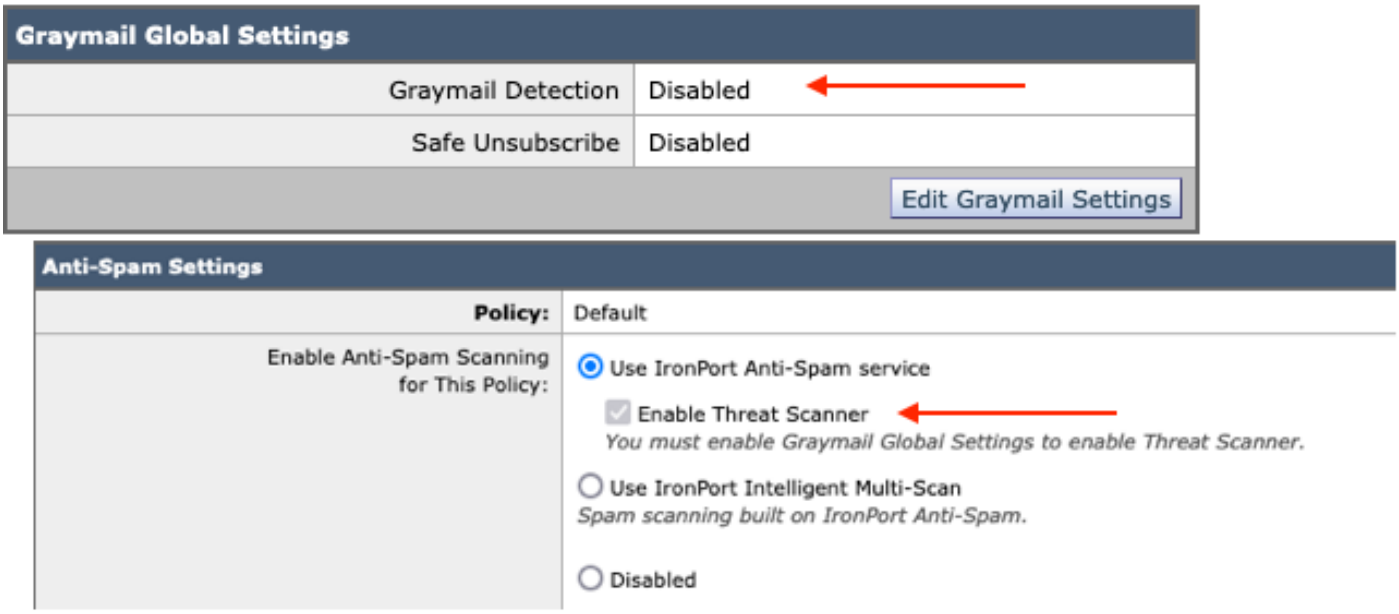
A configuração consiste em duas ações: Ativar detecção de e-mail de cinza e Ativar TS nas Políticas de e-mail de entrada.

- O serviço global do Graymail deve estar ativado para ativar o TS.
- A opção "Antispam" de política de e-mail de entrada para "Ativar mecanismo de varredura de ameaças" fica disponível quando o Graymail é ativado globalmente.

Configuração da interface da Web

Para ativar o Graymail na WebUII:

- Navegue até Serviços de segurança
    - IMS e Graymail
        - Configurações globais do Graymail
            - Editar configurações do Graymail.
                - Selecione a opção para ativar a Detecção de mensagens de cinza.
- Envie e confirme as alterações para finalizar a ação.

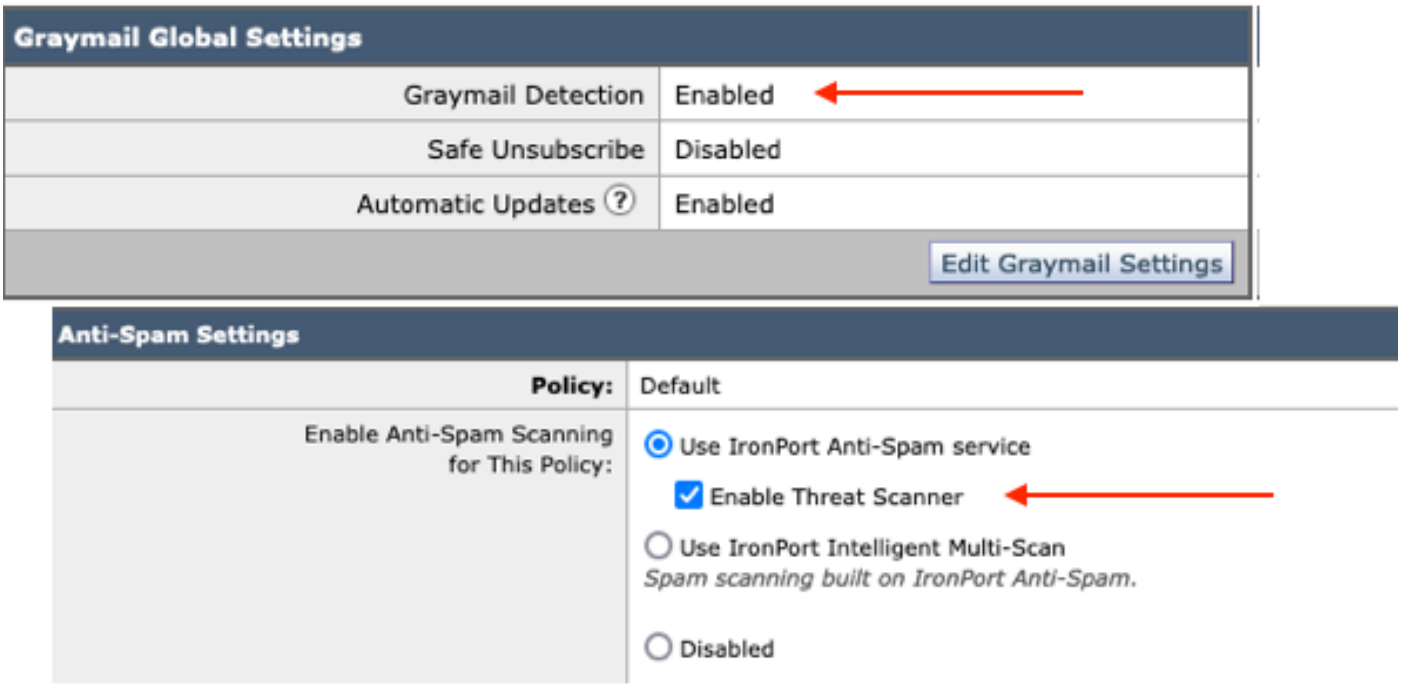


A visualização antes da configuração

Depois que o Graymail for ativado, a caixa de seleção Threat Scanner ficará disponível para cada Incoming Mail Policy (Política de recebimento de e-mails).

Para ativar o Threat Scanner na WebUI:

- Navegue até Políticas de e-mail
  - Políticas de recebimento de e-mail
    - Selecione a política de e-mail desejada
      - Selecione Anti-Spam.
        - A parte superior da página de configuração apresenta a opção de caixa de seleção para Ativar o Threat Scanner.
- Enviar e confirmar as alterações para finalizar a configuração



Opção de varredura de ameaças no Antispam

Configuração da interface de linha de comando

Ative o serviço do Graymail usando os comandos CLI.

- imsandgraymailconfig
  - mensagem de cinza
    - instalação
      - Deseja usar a Detecção de Correio de Cinza? [S] >
        - Deseja habilitar atualizações automáticas para o mecanismo do Graymail? [S]>
  - Preencha os prompts restantes para retornar ao prompt principal da máquina.

- Confirmar + adicionar comentários desejados > Concluir a ação pressionando a tecla "Return".

Ativando ou desativando o Threat Scanner em uma política a partir da CLI.

- CLI> policyconfig

Deseja configurar a Política de Emails Recebidos ou de Emails Enviados ou Corresponder à Prioridade de Cabeçalhos?

1. Políticas de recebimento de e-mail
2. Políticas de envio de e-mail
3. Corresponder Prioridade de Cabeçalhos

[1]> 1

Configuração de Política de Correio Recebido

1. Norte1
2. LISTA_BLOQUEADA
3. ALLOWED_LIST
4. ALLOW_SPOOF
5. INCUMPRIMENTO

Digite o nome ou número da entrada que deseja editar:
[]> 1

Escolha a operação que deseja executar:
- NAME - Alterar nome da política
- NOVO - Adicionar uma nova linha de membro de política
- DELETE - Remove uma linha de membro de política
- PRINT - Imprimir linhas de membros da política
- ANTISPAM - Modificar política antisspam
- ANTIVÍRUS - Modificar política de antivírus
- OUTBREAK - Modificar política de Filtros de Epidemia
- ADVANCEDMALWARE - Modificar a política de Proteção avançada contra malware

- GRAYMAIL - Modificar política do Graymail
- THREATDEFENSECONNECTOR - Modificar o conector de defesa contra ameaças
- FILTROS - Modificar filtros
[]> antispam

Escolha a operação que deseja executar:
- DISABLE - Desabilitar a política antisspam (Desabilita todas as ações relacionadas à política)
- ENABLE - Habilitar política antisspam
[]> habilitar

Iniciar configuração de antisspam

Deseja usar o Intelligent Multi-Scan nesta política? [N]>

Deseja usar o Antisspam IronPort nesta política? [S]>

Algumas mensagens são identificadas positivamente como spam. Algumas mensagens são identificado como spam suspeito. Você pode definir o Spam suspeito de antisspam IronPort Limite abaixo.
As opções de configuração aplicam-se a mensagens identificadas POSITIVAMENTE como spam:
Deseja habilitar tratamento especial para o veredito do Verificador de Ameaças? [N]> y

Continue pelas seleções de menu para concluir as opções de Política de e-mail e pressione a tecla "return" para aceitar a ação padrão para cada opção.

Conclua o salvamento com os comandos.

- Confirmar + adicionar comentários desejados > Concluir a ação pressionando a tecla "Return".

Verificar

Como ler e interpretar os registros.

O registro de e-mails do mecanismo de varredura de ameaças apresenta apenas um veredito provisório, enquanto CASE apresenta o veredito final.

Os registros de e-mail mostram duas verbidades diferentes para veredictos do verificador de ameaças limpos versus condenados

- Se o veredito Provisório do Verificador de Ameaças estiver limpo, o registro será apresentado da mesma forma que essas amostras.
    - Informações: veredito interino de mensagens em cinza - LEGIT (0) <Mensagem limpa>
    - Info: veredito interino pelo correio de cinza - MCE (11) <Campanha de e-mail diversa>
- Se o veredito provisório do Threat Scanner for condenar, o registro será apresentado da

mesma forma que essas amostras.
- Informações: veredito provisório do ThreatScanner - PHISHING (101)
- Informações: veredito provisório do ThreatScanner - VÍRUS (2)

Exemplo de logs de e-mail: o veredito de limpeza do mecanismo de varredura de ameaças usa um veredito diferente: veredito de e-mail cinza.

<#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
```

O Rastreamento de mensagens não mostra a entrada do log do Verificador de ameaças, apenas o CASE: Veredito final.

Esses exemplos do Threat Scanner (TS) apresentam os quatro cenários de veredito.

Observação: as categorias TS de "PHISHING" e "VÍRUS" são a única detecção que aumenta o peso do veredito do CASO

Exemplo de logs de e-mail: a condenação de PHISHING TS e a condenação de antisspam estão presentes

<#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
```

Amostra de rastreamento: a condenação de PHISHING TS está ausente e a condenação de CASE está presente.

PHISHING TS Condenado e Controle AntiSpam Condenado

Exemplo de logs de e-mail: a condenação de PHISHING TS e a negação de antisspam estão presentes.

<#root>

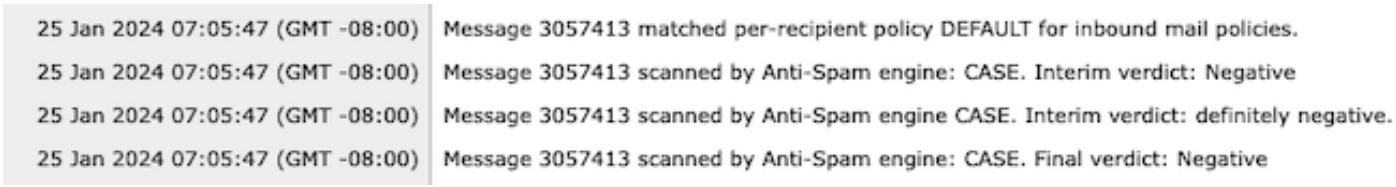
```
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

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

Exemplo de rastreamento: PHISHING TS Condenado e AntiSpam Negativo está presente.



Exemplo de logs de e-mail: exemplo de condenação de VÍRUS TS e antisspam dos logs de e-mail.

<#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
```

Exemplo de rastreamento: VÍRUS Condenação de TS ausente e Condenação de 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

Exemplo de logs de e-mail: VÍRUS TS Conviction e AntiSpam Negative estão presentes.

<#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
```

Amostra de rastreamento: VÍRUS TS Convicção ausente e AntiSpam Negativo 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

Os logs do Graymail contêm o veredito do Threat Scanner e o conteúdo de suporte para a análise do TALOS se for feito um desafio de falsos positivos.

A presença dos resultados brutos do Threat Scanner fez com que o registro do Graymail fosse sobreposto mais rapidamente. Para lidar com esse comportamento, as modificações de SEG foram feitas nos Logs do Graymail.

- O AsyncOS 15.5 define a Inscrição de log padrão para arquivos de log do Graymail como 20 para aumentar a retenção de log.
  - Nenhuma configuração de arquivo de log será alterada se a configuração for superior a 20 na atualização.
- As mensagens de entrada condenadas provisórias do Graymail exibem os resultados brutos da varredura completa, no Nível de informação.
- Os resultados da varredura de e-mail de cinza de todas as outras mensagens são exibidos no Nível de depuração.

Informações Relacionadas

- Guia de configuração do Email Security
- Página inicial do Cisco Secure Email Gateway para guias de suporte

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.