Configurar lista de exceções de domínio de remetente para Secure Email Gateway

Contents

Introdução

Este documento descreve "Novas alterações" na opção de configuração SDR (Sender Domain Reputation) Lista de exceções de domínio, para o Cisco Secure Email Gateway (SEG).

Contribuição de Chris Arellano, engenheiro do Cisco TAC.

Pré-requisitos

É desejável ter um conhecimento geral das definições e da configuração do SEG.

AsyncOS 15.0 e mais recente para Cisco Secure Email Gateway (SEG).

Compreensão geral do recurso SDR.

Requisitos

Ative o serviço de reputação de domínio do remetente e crie uma lista de endereços com a opção Somente domínio.

Componentes Utilizados

- As informações neste documento são baseadas nestas versões de software e hardware:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e mais recente.
- Reputação de domínio de remetente SEG.
- Address List (Lista de endereços).

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

A Reputação de domínio de remetente é um serviço em nuvem que coleta vários valores de remetente, obtém vereditos e fornece opções para agir sobre esses vereditos. O SDR permite que as configurações ignorem domínios confiáveis por meio do uso de uma Lista de Endereços aplicada à Lista de Exceções de Domínio.

A lista de exceções de domínio SDR nas versões AsynOS anteriores à SEG 15.0 tinha duas opções:

- Enabled = Faça a correspondência do envelope de, domínio para ignorar a ação do SDR.
- Desativado = Corresponder somente se todos estiverem presentes: Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC .

A lista de exceções de domínio para SEG 15.0 e opções mais recentes:

- Enabled = Faça a correspondência do envelope de, domínio para ignorar a ação do SDR.
- Desativado = Corresponder se o domínio estiver presente em qualquer um dos valores:
    - SAUDAÇÃO
    - RDNS
    - Envelope de
    - De
    - Responder para

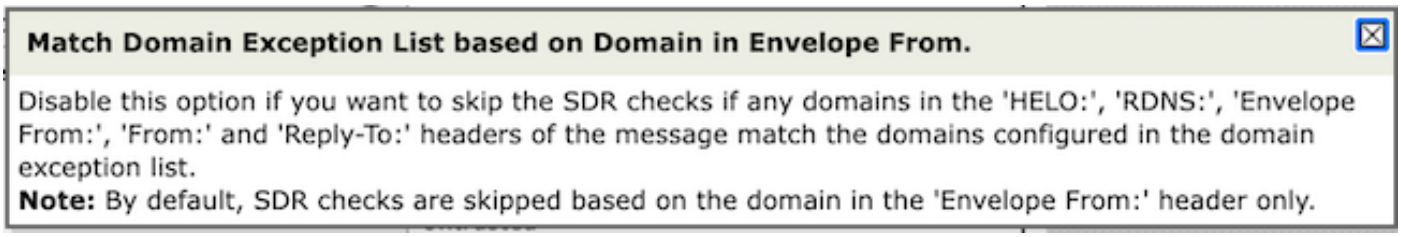
Configurar

O foco deste artigo é apenas a nova configuração da Lista de exceções de domínio. A instalação e a configuração completas do SDR são fornecidas no Guia do usuário.

Navegue na WebUI para Security Services > Domain Reputation.

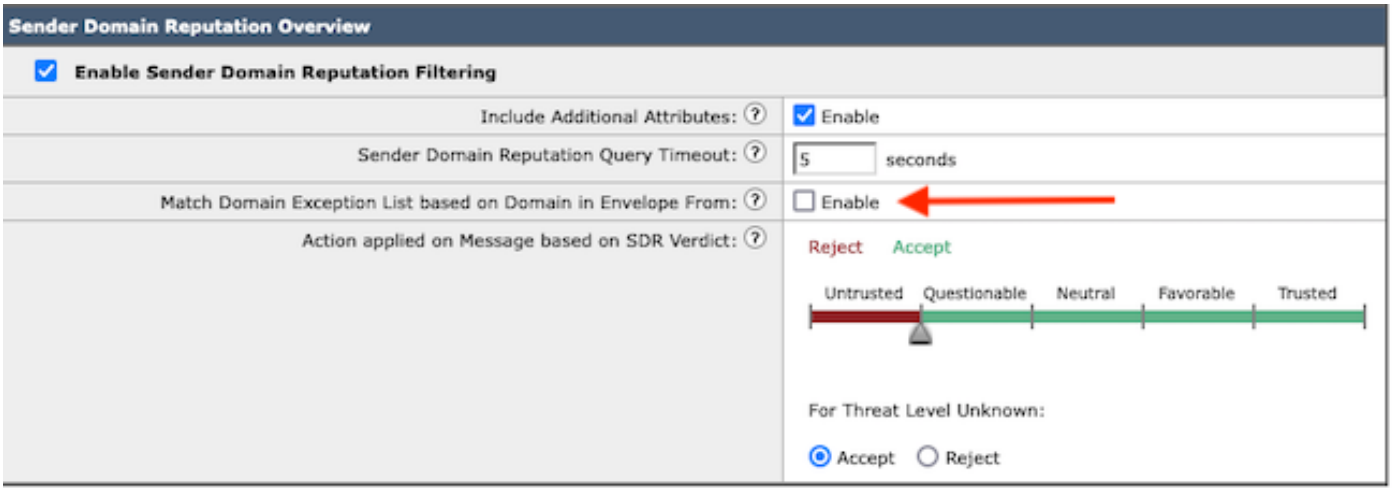
- A opção Match Domain Exception List com base na parte Domain Name do Envelope From é ativada por padrão.
    - Se a caixa de seleção estiver habilitada, apenas o valor "Envelope de, cabeçalho" corresponderá e ignorará a mensagem se condenada.
    - Se a Caixa de seleção estiver em branco, a Lista de exceções de domínio do SDR corresponderá a qualquer um destes campos de cabeçalho 'HELO:', 'RDNS:', 'Envelope De:', 'De:' e 'Responder Para:', corresponderá e ignorará a mensagem se for condenada.

Se o ícone informativo associado ? estiver selecionado, os detalhes da configuração serão apresentados.



Observação: por padrão, as verificações do SDR são ignoradas com base no domínio somente no cabeçalho 'Envelope de:'.

Selecione Edit Global Settings para remover a opção de caixa de seleção, como mostrado na imagem:



A própria Lista de Exceções de Domínio é uma Lista de Endereços que contém nomes de domínio.

Verificar

Para verificar o funcionamento correto usando a nova funcionalidade Desativar, você precisa de uma mensagem de teste enviada ao SEG com um valor de domínio correspondente em um dos 5 valores de cabeçalho.

Um log de exemplo que indica uma exceção na Lista de exceções global e correspondeu em uma Política de fluxo de e-mail seria apresentado no estágio inicial para os mail_logs:

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

Um log de exemplo que indica uma exceção conterá o domínio e o nome da lista de exceções.

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

Troubleshooting

Se surgirem dúvidas quanto à precisão de um veredito de mensagem selecionado, os valores serão documentados e comparados com o rastreamento de mensagem.

- Documente as Configurações globais do Domain Reputation > Configurações de segurança > Reputação de domínio.
- Verifique a Lista de endereços associada configurada nas Configurações globais do Domain Reputation.
- Verifique a Política de fluxo de e-mail correspondente com base no controle de mensagens.
- Verifique e anote os detalhes de quaisquer filtros de mensagens ou filtros de conteúdo com listas de exceção de domínio configuradas.

Colete o Rastreamento de mensagens, logs de e-mail e os cabeçalhos de e-mail originais.

- Se a exceção global corresponder a uma mensagem, não haverá entradas de log para a reputação do domínio, simplesmente uma linha indicando o domínio correspondente.
- Se a Lista de exceções global não corresponder a uma mensagem, há entradas de log para a Reputação de domínio a partir das quais os valores serão comparados.
    - Informações: MID 16 SDR: Domínios para os quais o SDR é solicitado: host DNS reverso: Não Presente, helo: mail1.example.com, env-from: test2.example.com, header-from: te
      destination.example.com, reply-to: test2.example.com
- Os cabeçalhos de e-mail incluem qualquer um dos 5 valores presentes em um e-mail individual para comparação com as configurações.

Quando todos os dados forem coletados, verifique se há correspondências ou ausência de correspondências para determinar a funcionalidade apropriada.

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.