Quarantine mensagens de Email falsificado no ESA e crie exceções para os remetentes que são permitidos ao spoof.

Índice

Introdução

Este documento descreve como controlar a falsificação do email em Cisco ESA e como criar exceções para que os usuários enviem email falsificado.

Pré-requisitos

Requisitos

Seu ESA deve processar ambos os correios entrantes/que parte e deve usar uma configuração padrão de RELAYLIST para embandeirar mensagens como que parte.

Componentes Utilizados

A informação neste documento é baseada no ESA com toda a versão de AsyncOS. 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Os componentes específicos usados incluem:

- **Dicionário**: usado para armazenar todos seus domínios internos.
- **Filtro da mensagem**: usado para segurar a lógica do email falsificado e de tratar da quarentena as exceções.
- **Quarentena da política**: usado para armazenar temporariamente email falsificado antes de decidir liberar-se, ou entregar, a mensagem. Considere adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT de mensagens liberadas ao WHITELIST para impedir mensagens futura deste remetente de incorporar a quarentena da política.
- **WHITELIST**: aliste provendo seus endereços IP de Um ou Mais Servidores Cisco ICM NT de emissão confiados. Adicionar um endereço IP de Um ou Mais Servidores Cisco ICM NT de um remetente a esta lista saltará a quarentena e permitirá o remetente ao spoof. Nós estamos colocando remetentes confiados em seu WHITELIST Sendergroup de modo que as mensagens falsificado destes remetentes não quarantined.
- **RELAYLIST**: aliste para os endereços IP de Um ou Mais Servidores Cisco ICM NT de autenticação que são permitidos retransmitir, ou envie o email de partida. Se o email está sendo entregado através deste sendergroup a suposição é que a mensagem não é uma mensagem falsificado.

  Nota: Se o sendergroup é chamado algo diferente do que **WHITELIST** ou **RELAYLIST** você terá que alterar o filtro com o nome correspondente do sendergroup. Igualmente se você tem ouvintes múltiplos, você pode igualmente ter mais de um WHITELIST.

Informações de Apoio

A falsificação é permitida à revelia em Cisco ESA. Há diversos motivos válidos para permitir que outros domínios enviem sobre seu interesse. Você pôde querer considerar controlar email falsificado quarantining mensagens falsificado antes que estejam entregadas, por exemplo.

Para tomar uma ação específica tal como a quarentena no email falsificado, você deve primeiramente detectar o email falsificado.

Que é falsificação do email?

A falsificação do email é a criação dos mensagens de Email com um endereço forjado do remetente.

Como detectar o email falsificado?

Você quererá filtrar todas as mensagens que tiverem um remetente do envelope (correio-de) e “amigável” (de) do encabeçamento que contém um de seus próprios domínios entrantes no endereço email.

Como permitir a falsificação para remetentes específicos?

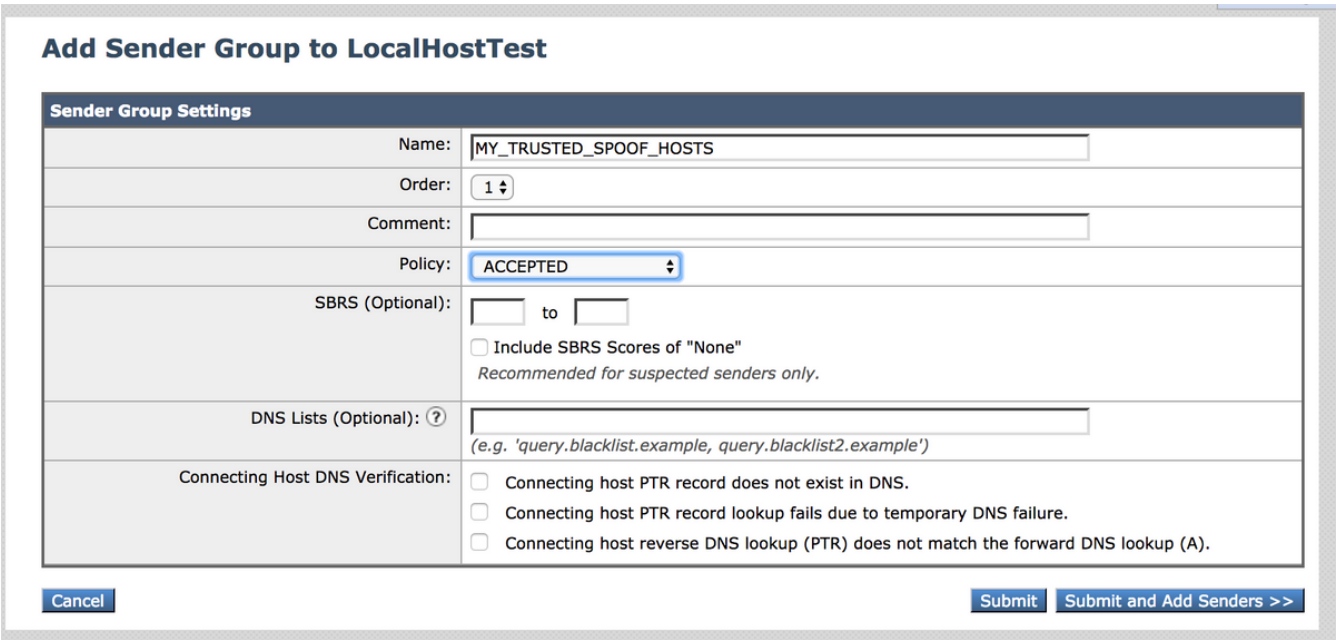
Quando executar o filtro da mensagem nestas mensagens artcile, falsificado for enviada à quarentena da política. Para adicionar uma exceção, adicionar simplesmente o IP do remetente ao WHITELIST.

Configurar

Crie o dicionário

de todos seus domínios para que você quer desabilitar a falsificação no ESA

- No GUI, navegue **para enviar políticas > dicionários.**
- O clique **adiciona o dicionário.**
- No campo de nome especifique **VALID_INTERNAL_DOMAINS**, por exemplo.
- Sob adicionar termos, adicionam todos os domínios para que você gostaria de desabilitar a falsificação.
- **Submeta e comprometa mudanças.**
-



Crie o filtro da mensagem

Para leverage o dicionário **VALID_INTERNAL_DOMAINS**

Conecte ao console do comando line interface(cli) de seu dispositivo e entre nos **filtros do** comando para obter o menu dos fiters da mensagem.

Cole e entre no filtro da mensagem abaixo.

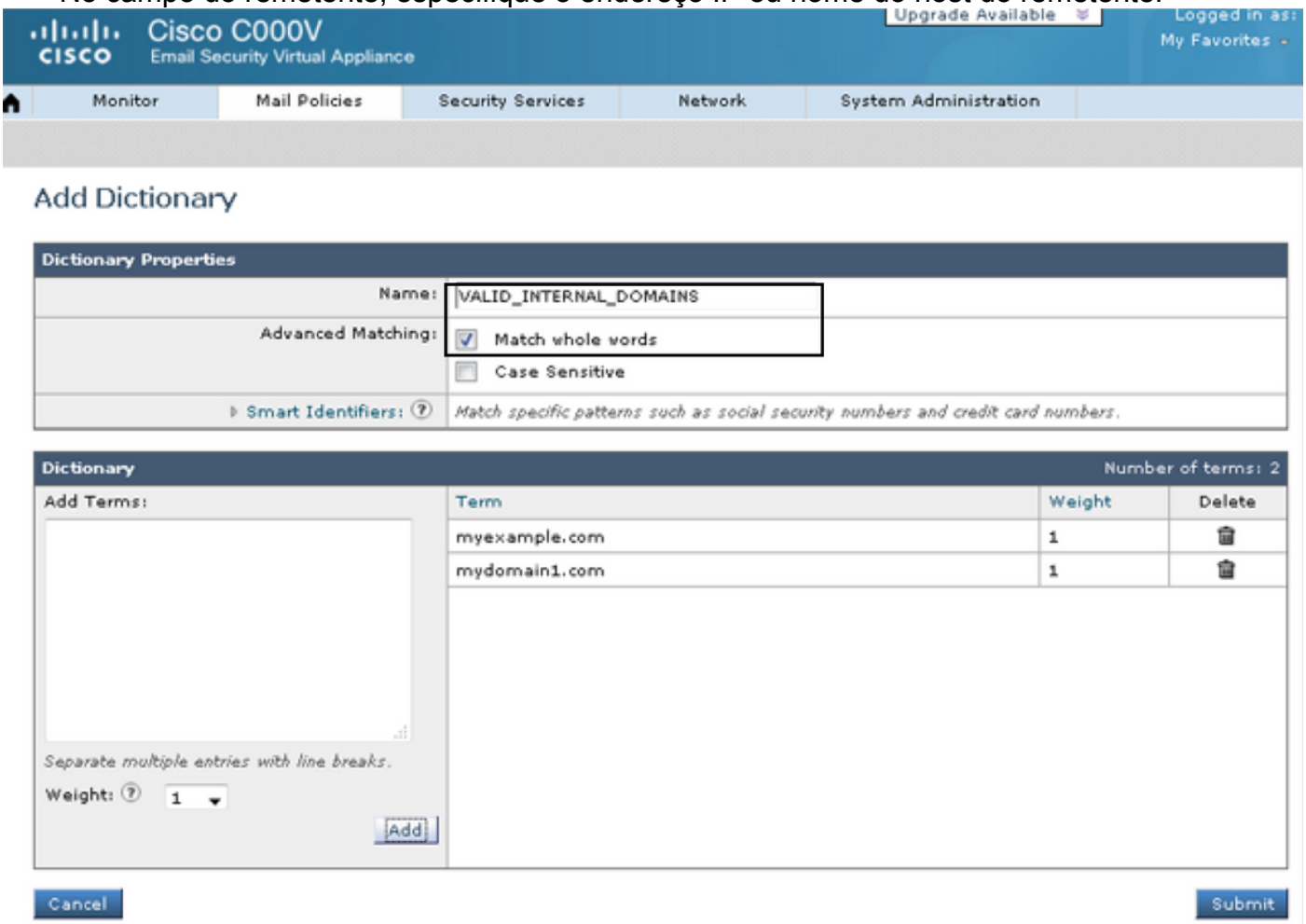
```
>filters
...
[]> new

Enter filter script.  Enter '.' on its own line to end.

quarantine_spoofed_messages: if ((mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1)) OR
(header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1))) AND ((sendergroup != "RELAYLIST")
AND (sendergroup !=
"WHITELIST")) {
                                quarantine("Policy");
                            }
.
1 filters added.
```

Submeta e comprometa mudanças

```
>commit
```

Adicionar Spoof-exceções ao WHITELIST

- Navegue às **políticas do correio** GUI **> à vista geral do CHAPÉU.**
- Abra o **WHITELIST** Sendergroup.
- No campo do remetente, especifique o endereço IP ou nome do host do remetente.



Submeta e comprometa mudanças

```
>commit
```

Verificar

Verifique que as mensagens falsificado Quarantined

Envie um mensagem de teste que especifica um de seus domínios como o remetente do envelope. Valide o filtro está trabalhando como esperado executando uma trilha da mensagem nessa mensagem. O resultado esperado é que a mensagem obterá quarantined porque nós não criamos nenhuma exceções contudo para aqueles remetentes são permitidos que ao spoof.

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <sbayer@cisco.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <sbayer@cisco.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
```

```
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message
filter:quarantine_spoofed_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Verifique que mensagens da Spoof-exceção está sendo entregada

Os remetentes da “Spoof-exceção” são endereços IP de Um ou Mais Servidores Cisco ICM NT em seus sendergroups providos no filtro acima.

RELAYLIST é provido porque é usado pelo ESA para enviar o correio de partida. As mensagens que estão sendo enviadas por RELAYLIST são correio tipicamente de partida, e não incluir isto criaria falsos positivos, ou mensagens externa que estão sendo quarantined pelo filtro acima.

Exemplo do rastreamento de mensagem de um endereço IP de Um ou Mais Servidores Cisco ICM NT da “Spoof-exceção” que fosse ao WHITELIST. A ação prevista sido entrega e não quarantine. (Este IP é permitido ao spoof)

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <sbayer@cisco.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <sbayer@cisco.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <sbayer@cisco.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598 Message accepted
for delivery'
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Informações Relacionadas

Filtração falsificado do correio ESA

Proteção do spoof usando a verificação do remetente