Criando uma política de Whitelist em Cisco ESA para testes da educação do phishing

Índice

Introdução

Este documento descreve como criar uma política de Whitelist no exemplo da Segurança do email da ferramenta de segurança (ESA) ou da nuvem do email de Cisco (CES) para permitir testes/campanhas da educação do phishing.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Navegando e configurando regras em Cisco ESA/CES no WebUI.
- Criando filtros da mensagem em Cisco ESA/CES no comando line interface(cli).
- Conhecimento do recurso usado para a campanha/teste do phishing.

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.

Informações de Apoio

Os administradores que executam testes ou campanhas da educação do phishing terão email gerados com informação que será combinada contra as regras atuais de Talos nos grupos da regra de filtro do Anti-Spam e/ou da manifestação. Em tal evento, os email da campanha do phishing não alcançarão utilizadores finais e actioned por Cisco ESA/CES próprio que causa assim o teste a uma parada. Os administradores precisariam de assegurar-se de que o ESA/CES permitisse através destes email de realizar seus campanha/teste.

Configurar

aviso: A posição de Cisco em vendedores whitelisting da simulação & da educação do phishing não é permitida globalmente. Nós recomendamos administradores trabalhar com o serviço do simulador do phishing *(por exemplo: PhishMe)* para obter seu IPs adicionar-lo então localmente ao Whitelist. Cisco deve proteger nossos clientes ESA/CES daqueles IPs se mudam nunca as mãos ou se transformam realmente uma ameaça.

Cuidado: Os administradores devem somente manter estes IPs em um Whitelist ao testar, deixar o IPs externo em uns testes do cargo de Whitelist por um período de tempo prolongado pode trazer espontâneo ou os email maliciosos aos utilizadores finais estes IPs tornam-se comprometidos.

Na ferramenta de segurança do email de Cisco (ESA), crie um grupo novo do remetente para sua simulação do phishing e atribua-o à política do fluxo de correio $TRUSTED. Isto permitirá que todos os email da simulação do phishing sejam entregados aos utilizadores finais. Os membros deste grupo novo do remetente não são sujeitos avaliar a limitação, e o índice daqueles remetentes não é feito a varredura pelo motor do Anti-Spam de Cisco IronPort, mas é feito a varredura ainda pelo software anti-vírus.

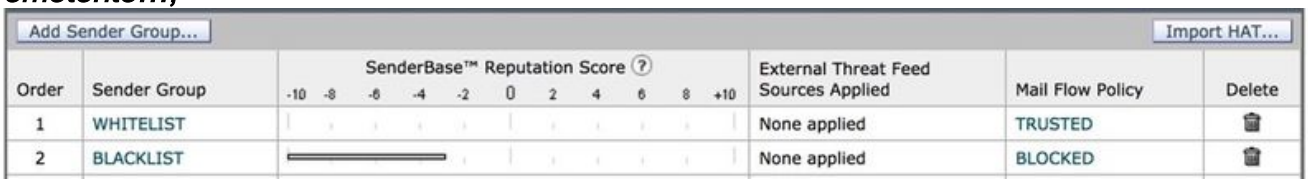
Nota: À revelia, a política do fluxo de correio $TRUSTED tem permitida anti-vírus mas o Anti-Spam desligados.

Criando o grupo do remetente

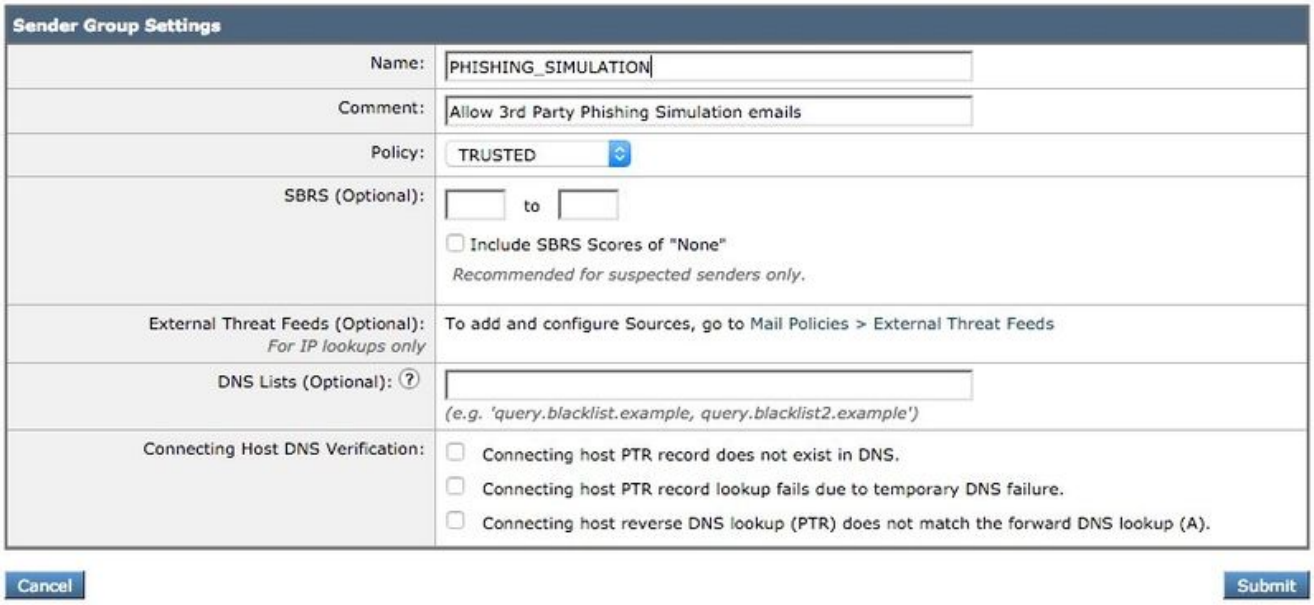
1. Clique a aba das ***políticas do correio***.
2. Sob a seção da ***tabela do acesso host***, selecione a ***vista geral do CHAPÉU***

3. À direita, certifique-se que seu ouvinte de ***InboundMail*** está selecionado atualmente,
4. Da coluna do ***grupo do remetente*** abaixo, o clique ***adiciona o grupo do***

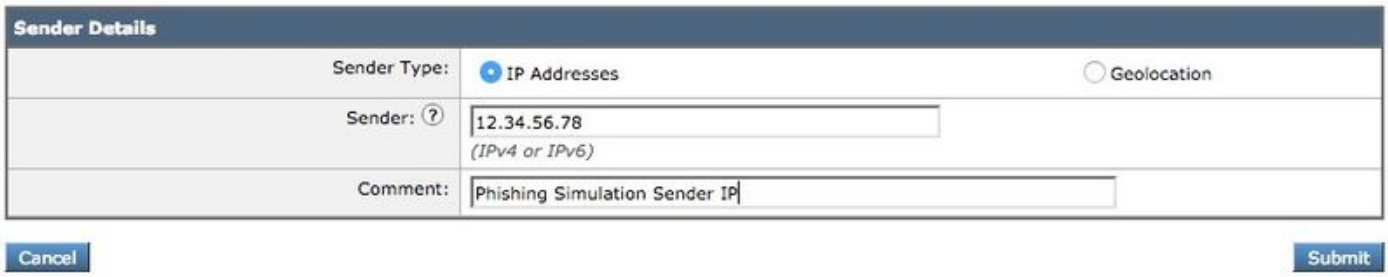
remetente…,



5. Preencha o ***nome*** e os ***campos de comentário***. Sob a ***política*** dropdown, "**$TRUSTED** seletos" e clicam então ***submetem e adicionam remetentes >>.***



6. Entre no IP ou no hostname que você quer a Whitelist no primeiro campo. Seu sócio da simulação do phishing fornecê-lo-á a informação IP do remetente.



Quando você termina adicionar entradas, clique o ***botão Submit Button***. Recorde clicar as ***mudanças comprometer*** abotoam-se para salvar suas mudanças.

Criando o filtro da mensagem

Após ter criado o grupo do remetente para permitir o desvio do Anti-Spam e anti-vírus, um filtro da mensagem é exigido para saltar os outros motores da Segurança que podem combinar a campanha/teste do phishing.

1. Conecte ao CLI do ESA.
2. Execute os ***filtros do*** comando.
3. Execute o comando new criar um filtro novo da mensagem.
4. A cópia e cola o seguinte exemplo do filtro, fazendo edita para seus nomes do grupo reais

do remetente se necessário:

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. Retorne à alerta principal CLI e pressione entram.
6. Seja executado *comprometem* para salvar a configuração.

Verificar

Use o recurso da terceira para enviar uma campanha/teste do phishing e para verificar os resultados nos logs do rastreamento de mensagem para assegurar todos os motores foram saltados e o email foi entregado.