Melhores prática da configuração para CES ESA

Índice

Introdução

Este documento fornece um sumário das recomendações para os administradores que usam a Segurança do email da nuvem de Cisco (CES) para configurar seu Cisco envia por correio eletrónico a ferramenta de segurança (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- A administração ESA, a administração do nível CLI e GUI

Componentes Utilizados

A informação neste documento é baseada em melhores prática e em recomendações para clientes e administradores CES.

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.

Produtos Relacionados

Este documento pode igualmente ser usado com estes versão de hardware e software:

- Hardware de em-locais ESA e dispositivos virtuais (NON-CES) que executam alguma versão de AsyncOS para a Segurança do email

Melhores prática da configuração para CES ESA

> **aviso:** Todas as mudanças às configurações baseadas nos melhores prática da maneira prevista neste documento devem ser revistas e compreendido antes de comprometer suas alterações de configuração em um ambiente de produção. Consulte por favor com seu engenheiro de sistema ou equipe de conta CES antes de fazer as alterações de configuração que você 100% não compreende nem tem o conforto com ao administrar.

Serviços de segurança

Anti-Spam de IronPort (IPA)

- Sempre o 1.5 MB da varredura e nunca faz a varredura do 2 MB

Filtragem URL

- Permita a categorização e a reputação URL
- Permita o seguimento da interação da Web

Detecção de Graymail

- Permita e 1 MB máximo do tamanho das mensagens

Filtros da manifestação

- Permita regras adaptáveis, 1 MB máximo do tamanho da varredura
- Permita o seguimento da interação da Web

Proteção avançada do malware

- Permita tipos de arquivo adicionais após ter permitido a característica

Rastreamento de mensagem

- Permita o registro rejeitado da conexão (se for necessário)

A administração do sistema

Usuários

- Ajuste políticas de senha
- Se Lightweight Directory Access Protocol (LDAP) possível da força de alavanca para a autenticação

Assinaturas do log

- Permita logs do histórico de configuração
- Permita logs da Filtragem URL
- Registre o encabeçamento adicional “de”

Mudanças de nível CLI

Filtragem URL da Segurança SD da Web

- **websecurityadvancedconfig**

```
Do you want to disable DNS lookups? [N]> y

Enter the maximum number of URLs that should be scanned:
[100]> 20

Enter the threshold value for outstanding requests:
[50]> 5

Enter the default time-to-live value (seconds):
[30]> 600

Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

Registro URL

- ESA permitindo a Filtragem URL e os melhores prática
- **outbreakconfig**

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

Filtro do Anti-spoof

- Detecção forjada do email (ALIMENTADA) com Segurança do email de Cisco

Encabeçamento que carimba o filtro

- escreva e permita o filtro do seguinte mensagem:

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Tabela do acesso host

Grupos adicionais do remetente

- Guia do Usuário ESA: Criando um grupo do remetente para o manejo de mensagem
  SKIP_SBRS – Coloque mais altamente para as fontes que saltam a reputaçãoSPOOF_ALLOW – Parte de filtro da falsificaçãoSÓCIO – Para conexões forçadas

TLS

No grupo predefinido do remetente SUSPECTLIST

- Guia do Usuário ESA: Verificação do remetente: Host permita “contagens SBR em nenhuns”Opcionalmente, permita “conectando o host a consulta do registro que PTR falha devido à falha de DNS provisória”

Amostra agressiva do CHAPÉU

- LISTA NEGRA [-10 à POLÍTICA -2]: OBSTRUÍDO
- SUSPECTLIST [-2 à POLÍTICA -1]: HEAVYTHROTTLED
- GRAYLIST[-1 a 2 e NENHUNS] POLÍTICA: LIGHTTHROTTLED
- ACCEPTLIST [2 à POLÍTICA 10]: ACEITO

Nota: Os exemplos acima do CHAPÉU mostram políticas adicionalmente configuradas do fluxo de correio. Para obter informações completas sobre de MFP, refira por favor o Guia do Usuário da versão apropriada de AsyncOS para a Segurança do email que é executado em seu ESA. Exemplo, AsyncOS 10.0: Tabela do acesso host (CHAPÉU), grupos do remetente, e políticas do fluxo de correio

Política do fluxo de correio (parâmetros da política padrão)

Configurações de segurança

- Ajuste o Transport Layer Security (TLS) ao preferido
- Permita a estrutura de política do remetente (o SPF)
- Permita o correio identificado DomainKeys (DKIM)
- Enable Domínio-baseou a autenticação de mensagem, o relatório e a verificação da conformidade (DMARC) e envia relatórios agregados do feedback

Nota: DMARC exige o ajustamento adicional a configurar. Para obter informações completas sobre de DMARC, refira por favor o Guia do Usuário da versão apropriada de AsyncOS para a Segurança do email que é executado em seu ESA. Exemplo, AsyncOS 10.0: Verificação DMARC

Políticas do correio recebido

Pontos iniciais do Anti-Spam

- Os pontos iniciais devem ser deixados em pontos iniciais do padrão. A alteração de marcar podia conduzir a um aumento do falso positivo.

Anti-vírus

- Exploração da mensagem: Varredura para vírus somente
- As mensagens de Unscannable, vírus contaminaram mensagens: ajuste do “o mensagem original arquivo” ao nenhum

Ampère

- Adicionar o “ampère” para sujeitar Prepend para Unscannable, desabilitação do “mensagem arquivo”

Graymail

- A exploração permitida para cada sentença, Prepend o assunto e entrega-o
- Adicionar o x-encabeçamento para o email maioria, encabeçamento = “X-BulkMail”, valor = “verdadeiro”

Filtros da manifestação

- O nível da ameaça do padrão é 3, ajusta por favor conforme seus requisitos de segurança Se a ameaça em nível para uma mensagem iguala ou excede este ponto inicial, a mensagem estará enviada à quarentena da manifestação. (ameaça 1=lowest, ameaça 5=highest)
- Permita a alteração da mensagem. Reescreva a URL para mensagem sem assinatura
- O assunto da mudança prepend a: [Possible $threat_category Fraud]

Políticas que parte do correio

Anti-vírus

- Exploração da mensagem
- Varredura para vírus somentea un-verificação inclui um X-encabeçamento com os resultados de exploração AV na mensagem
- Para todas as mensagens: Avançado > a outra notificação, permite “outro” e inclui o endereço email do contato admin/SOC

Quarentena da política

PRE-crie as seguintes quarentena:

- De entrada impróprio
- De partida impróprio
- De entrada malicioso URL
- De partida malicioso URL
- Spoof suspeito
- Malware

Outros ajustes

Dicionários

- Permita/profanidade da revisão e dicionário sexual dos termos
- Crie o dicionário forjado do email com os nomes executivos
- Crie o dicionário para palavras-chaves restritas ou outras

Controles do destino

- Permita o TLS para o destino do padrão
- Ajuste limiares inferiores para domínios do webmail
- Limite de taxa seu próprio correio de partida com ajustes do controle do destino

Filtros satisfeitos

Nota: Para obter informações completas sobre dos filtros satisfeitos, refira por favor o Guia do Usuário da versão apropriada de AsyncOS para a Segurança do email que é executado em seu ESA. Exemplo, AsyncOS 10.0: Filtros satisfeitos

Filtro satisfeito impróprio

- A profanidade das circunstâncias OU o fósforo de dicionário sexual, enviam uma cópia à quarentena imprópria

Filtro malicioso do índice da reputação URL

- Envie uma cópia à URL maliciosa (-10 a -6) para quarantine

Filtro do índice da categoria URL com o estes selecionados

- Adulto, pornografia, pederastia, jogando
- Envie uma cópia à quarentena imprópria

Detecção forjada do email

- “Executives_FED nomeado dicionário”
- Quarentena do ponto inicial 90 FED() uma cópia

O macro permitiu o filtro satisfeito dos documentos

- se uns ou vários acessórios contêm um macro
- Condição opcional - > dos SBR não confiáveis varie
- Envie uma cópia para quarantine

Proteção do acessório

- se uns ou vários acessórios são protegidos
- Condição opcional - > dos SBR não confiáveis varie
- Envie uma cópia para quarantine

Informações Relacionadas

- BRKSEC-2131 - Cisco envia por correio eletrónico a Segurança: Melhores prática e ajuste fino (2016 Las Vegas)
- BRKSEC-2131 - Segurança do email para povos do NON-E-correio (2015 San Diego)
- BRKSEC-3770 - (DMARC) - não são uns phish: mergulho profundo em técnicas de autenticação do email (2014 San Francisco)
- Contrato de licença do utilizador final CES
- O CES presta serviços de manutenção à descrição
- Termos universais da nuvem de Cisco
- Suporte Técnico e Documentação - Cisco Systems