Erros da configuração comum no ESA

Índice

Introdução

Este documento descreve erros da configuração comum na ferramenta de segurança do email (ESA).

Que são os erros da configuração comum no ESA?

Se você está estabelecendo uma avaliação nova ou está olhando sobre uma configuração existente, você pode referir esta lista de verificação de erros da configuração comum.

1. CHAPÉU

- Não põe contagens positivas SBR como +5 ou +7 no WHITELIST. Uma escala de 9.0-10.0 seria APROVADA, mas incluir umas mais baixas contagens fá-la-á somente mais provavelmente que o Spam obterá completamente.

- Desabilite o UNKNOWNLIST, a verificação do remetente DNS do envelope e a conexão da verificação do host DNS a menos que você realmente precisar e compreender estes.

- Em vez do tamanho de mensagem em mudança e dos outros ajustes da política em cada política do fluxo de correio, vão ao menu de políticas do fluxo de correio e escolhem a última opção, da “os parâmetros política padrão”.

- Limite conexões máxima a três para a maioria de remetentes, e faça a isto o padrão para políticas novas do fluxo de correio.

- Certifique-se das contagens de SenderBase de -10.0 a -2.0 estejam incluídas na LISTA NEGRA. A documentação e os assistentes de configuração são excedentemente conservadores; nós não temos atualmente nenhum falso positivo nesta escala.

2. Política

- Nomeie políticas após quem o obtém, não o que faz. Nomeie todos os filtros satisfeitos após o que faz, e use abreviaturas como Q_basic_attachments, D_spoofers, Strip_Multi-Media, onde Q significa que a quarentena e D significam a gota.

- Políticas não-padrão se “use configurações padrão” para o Anti-Spam, o Anit-vírus, filtros satisfeitos e filtros da manifestação a não ser que onde você precisa realmente ajustes especiais. Não recreie aqueles ajustes em cada política se não é necessário.

- Untick “gota contaminou acessórios” ou então você passará sobre muitos email vazios onde o vírus foi descascado.

- Os ajustes anti-vírus para de partida devem notificar o remetente, não o receptor

- Os filtros e o Anti-Spam da manifestação devem ser desabilitados em de partida

3. Relés entrantes

Se o “monitor > a vista geral” mostram conexões de seus próprios server e domínios, você precisa de adicionar-los à instalação entrante dos relés. Muito um erro comum, ao usar o GUI, é pensar que você permitiu os novos recursos de relay quando tudo que você fez é adiciona as entradas à tabela. Além:

- Adicionar um grupo especial do remetente do CHAPÉU para elas, acima do WHITELIST, para relatar finalidades. Não escolha nenhum limitação da taxa ou DHAP, mas a detecção do Spam e do vírus é APROVADA.

- Adicionar um filtro da mensagem para combinar sua ação de política da LISTA NEGRA. Por exemplo:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

Em casos raros onde você está injetar novamente o email (por exemplo, re-processando o correio do inter-subscritor com a política de entrada do correio), seu filtro igualmente precisará de isentar a relação do reinjection. Normalmente isto não é necessário.

4. DNS

Muitos clientes forçam o ESA para perguntar seus servidores internos de DNS fora do hábito. Na maioria de instalações, 100% dos registros que DNS nós precisamos estão no Internet, não nos DN internos. Faz mais sentido perguntar os servidores root do Internet, reduzindo a carga da transmissão nos DN internos.

5. Filtros da mensagem e do índice

A maioria de erro comum é pôr circunstâncias de harmonização nos filtros satisfeitos onde não são exigidas. A maioria de filtros devem alistar algumas ações, mas a circunstância deve ser deixada vazia. O filtro será *verdadeiro* sempre, e será executado sempre. Você controla que os usuários/políticas recebem estas ações criando políticas entrantes ou que parte novas do correio como necessárias, e aplicando este filtro à política. Estão aqui os exemplos incorretos e corretos:

- Équase sempre um erro para usar RCPT-à circunstância em um filtro da mensagem. O procedimento correto é escrever um filtro satisfeito entrante, e faz específico para um usuário particular adicionando uma política receptor-baseada do correio recebido.

- Équase sempre um erro para ter um teste satisfeito do filtro para a presença de um acessório, a seguir deixa cair o acessório. O método correto é deixar cair sempre esse acessório, sem testar para sua presença.

- Équase sempre um erro para usar o deliver(). Entregue significa a faixa clara todos os filtros restantes, a seguir entregam-na. Se você apenas quer entregar sem saltar o resto dos filtros, nenhuma ação explícita está exigida (implicado entregue).

7. Abra a prevenção do relé

Alguns serviços verificarão para considerar se seu agente de transferência de mensagem (MTA) aceita os endereços que potencialmente poderiam conduzir a condições abertas do relé. Desde que deixar seu MTA como um relé aberto de funcionamento é ruim, estes locais podem adicionar-lo às listas negras a menos que você rejeitar estes endereços perigosos na conversação SMTP.

Adicionar um grupo especial do remetente do CHAPÉU para eles, acima do WHITELIST, para relatar finalidades. Não escolha nenhum limitação da taxa ou DHAP, mas permita a detecção do Spam e do vírus.

- Mude ao endereço restrito que analisa gramaticalmente (é frouxamente o padrão). Isto é necessário para impedir o dobro @ assina dentro endereços.

- Caracteres inválidos da rejeição (não tira). Isto é igualmente necessário para impedir o dobro @ assina dentro endereços.

- Rejeite (para não aceitar) literais, e incorpore os seguintes caráteres: *%! \ \/?

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems