Que são os melhores prática para usar SenderBase?

Índice

Introdução

Este documento descreve os melhores prática para usar SenderBase.

Que são os melhores prática para usar SenderBase?

O serviço da reputação de SenderBase (SBR) fornece um exato, a maneira flexível para que você rejeite ou estrangule os sistemas suspeitados transmitir o Spam baseado no endereço IP de Um ou Mais Servidores Cisco ICM NT de conexão do host remoto. Os SBR retornam uma contagem baseada na probabilidade que uma mensagem de uma fonte dada é Spam, variando de -10 (certo ser Spam) com 0 a +10 (certo não ser Spam). Embora os SBR possam ser usados como uma solução autônoma do anti-Spam, é a mais eficaz quando combinada com um varredor índice-baseado do anti-Spam.

As contagens de SenderBase podem ser usadas na tabela do acesso host (CHAPÉU) em um ouvinte S TP para traçar conexões SMTP entrantes aos grupos diferentes do remetente. Cada grupo do remetente associou com ele uma política que afetasse como o email entrante é segurado. As coisas as mais comuns a fazer com contagens de SenderBase são ao correio da rejeição inteiramente, ou para estrangular o remetente suspeitado do Spam.

Você pode usar contagens SBR no CHAPÉU para rejeitar ou estrangular o email. Você pode igualmente criar filtros da mensagem para especificar “pontos iniciais” para que as contagens SBR atuem mais em cima das mensagens processadas pelo sistema. O diagrama abaixo fornece um esboço áspero de como as contagens SBR podem ser usadas para obstruir ou estrangular remetentes suspeitados:

1. As filiais de SenderBase enviam o tempo real, dados globais.
2. Enviar o MTA abre a conexão com o dispositivo.
3. O dispositivo verifica dados globais para ver se há o endereço IP de Um ou Mais Servidores Cisco ICM NT de conexão.
4. O serviço da reputação de SenderBase calcula a probabilidade que esta mensagem é Spam

e atribui uma contagem das reputações de SenderBase.
5. O dispositivo retorna a resposta (rejeitando o email ou estrangulando o remetente) baseada na contagem da reputação de SenderBase.

Como você se usa as contagens SBR dependerão de como agressivo você quer estar no email defiltração. A ferramenta de segurança do email (ESA) oferece três estratégias diferentes para executar SenderBase:

- Conservador: Um abordagem conservadora é obstruir mensagens com uma contagem da reputação de SenderBase mais baixa de -7.0, estrangulá-lo entre -7.0 e -2.0, aplicar a política padrão entre -2.0 e +6.0, e aplicar a política confiada para mensagens com uma contagem maior de +6.0. Usar esta aproximação assegura uma taxa zero próxima do falso positivo ao conseguir o melhor desempenho de sistema.
- Moderado: Uma aproximação moderado é obstruir mensagens com uma contagem da reputação de SenderBase mais baixa de -4.0, estrangulá-la entre -4.0 e 0, aplicar a política padrão entre 0 e +6.0, e aplicar a política confiada para mensagens com uma contagem maior de +6.0. Usar esta aproximação assegura uma taxa muito pequena do falso positivo ao conseguir o melhor desempenho de sistema (porque mais correio é desviado longe do Anti-Spam que processa).
- Agressivo: Uma aproximação agressiva é obstruir mensagens com uma contagem da reputação de SenderBase mais baixa de -1.0, estrangulá-la entre -1.0 e 0, aplicar a política padrão entre 0 e +4.0, e aplicar a política confiada para mensagens com uma contagem maior de +4.0. Usando esta aproximação, você pôde incorrer alguns falsos positivos; contudo, esta aproximação maximiza o desempenho de sistema desviando a maioria de correio longe do processamento do Anti-Spam.

O gráfico e a tabela abaixo resumem estas três políticas:

Executando SenderBase que estrangula ou obstrução

A melhor maneira de usar contagens de SenderBase significa o seguimento de um simples, metodologia da 2-parte. Primeiramente, você decide em sua política (por exemplo, você poderia começar com a política “conservadora” acima) e traça essa política aos grupos do remetente. Então, você traça aqueles grupos do remetente à política que você quer. O ESA tem criado já uma matriz dos grupos do remetente e das políticas do fluxo de correio que podem servir como um molde para sua aplicação dos SBR.

Para executar o estrangulamento de SenderBase baseado na política padrão, você editará os quatro grupos do remetente (Whitelist, lista negra, Suspectlist, e Unknownlist) em políticas do correio > em vista geral da tabela do acesso host (CHAPÉU). Comece clicando no grupo do remetente de “Whitelist”. Então, usando o menu suspenso nos remetentes catalogue, clique sobre “adicionam o remetente” com de “a contagem da reputação SenderBase (SBR)” selecionada. Isto adicionará SBR alinha à lista de remetentes. Preencha sua escala da contagem SBR (neste caso 6.0 10.0) e clique o botão Submit Button.

A política para o grupo do remetente de Whitelist “é confiada. ” À revelia, esta política saltará o anti-Spam que processa, que aumentará o desempenho de sistema. Porque os remetentes com as contagens muito altas SBR são altamente pouco suscetíveis de enviar o Spam, esta etapa apenas aumentará a taxa de transferência. Edite os três grupos permanecendo do remetente

para adicionar contagens SBR, de acordo com a tabela abaixo:

Grupo do remetente	Escala da contagem	Resultado
Whitelist	6 a 10	Os bons remetentes conhecidos não serão feitos a varredura
Unknownlist	-2 a +6	Os remetentes com pouca informação serão feitos a varredura normalmente
Suspectlist	-7 a -2	Os remetentes com reputação deficiente serão estrangulados pesadamente p reduzir a quantidade de Spam que podem enviar
Lista negra	-10 a -7	O correio dos spammer conhecidos será rejeitado no tempo S TP com uma resposta 5xx

Quando você é feito que adiciona escalas da contagem, não esqueça clicar “**compromete mudanças**.” Quando você está adicionando SBR que marca regras aos grupos existentes do remetente, coloque-os na parte inferior da lista de remetentes em qualquer grupo. Peça matérias ao definir grupos do remetente no CHAPÉU de um ouvinte, como os grupos são avaliados de cima para baixo, e dentro de cada grupo, cada regra é avaliada individualmente, de cima para baixo. Em um CHAPÉU, a primeira regra que combina um remetente será usada para selecionar uma política. Se uma conexão recebida de um domínio de emissão tem SBR definidos marca e combina a escala em uma regra no CHAPÉU do ouvinte, a política do fluxo de correio será aplicado, mesmo se a outra pena mais adicional das regras na lista de grupos do remetente pôde igualmente combinar.

Se sua política para pôr remetentes em grupos do remetente exige que todas as regras NON-SBR estejam avaliadas antes que as contagens SBR estejam consideradas, a seguir você pode simplesmente adicionar quatro grupos novos do remetente na extremidade da lista de grupos existentes do remetente especificamente para a política SBR que combina junto com suas políticas relevantes.

Informações Relacionadas

- Perguntas mais frequentes de SenderBase
- Suporte Técnico e Documentação - Cisco Systems