

SenderBase funciona corretamente atrás do NAT?

Índice

[Introdução](#)

[SenderBase funciona corretamente atrás do NAT?](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve SenderBase e sua funcionalidade atrás do Network Address Translation (NAT) para a ferramenta de segurança do email de Cisco (ESA).

SenderBase funciona corretamente atrás do NAT?

SenderBase é um serviço com base em IP da reputação que atribua contagens do serviço da reputação de SenderBase (SBR) aos endereços IP de Um ou Mais Servidores Cisco ICM NT. SenderBase marca a escala de -10 a +10, que reflete a probabilidade que um endereço IP de Um ou Mais Servidores Cisco ICM NT de emissão tenta enviar a Spam. As contagens altamente negativas indicam os remetentes que são muito prováveis enviar o Spam; as contagens altamente positivas indicam os remetentes que são pouco suscetíveis de enviar o Spam.

O ouvinte S TP em um ESA faz SBR marca perguntas usando as perguntas DNS baseadas no endereço IP de Um ou Mais Servidores Cisco ICM NT da conexão de TCP entrante. Se o endereço IP de Um ou Mais Servidores Cisco ICM NT que o dispositivo do email vê é o endereço “real” do remetente, então os SBR funcionam como esperado.

Nota: Se um Firewall usa o NAT para o endereço IP de origem, não introduzirá um cabeçalho da mensagem novo que contenha o endereço IP de Um ou Mais Servidores Cisco ICM NT da fonte original. Sem um cabeçalho da mensagem que contenha o endereço IP original, os novos recursos de relay não trabalharão. Sem a informação de cabeçalho para o endereço IP de origem, o ESA não pode determinar o endereço IP de Um ou Mais Servidores Cisco ICM NT da fonte original.

A maioria de empresas que usam o NAT assim escondem endereços internos do Internet (ou porque não têm os suficientes endereços IP de Um ou Mais Servidores Cisco ICM NT a se operar sem uma função NAT ou NAPT). Nos casos, SenderBase trabalha com sucesso porque o endereço IP de Um ou Mais Servidores Cisco ICM NT do remetente externo não é alterado em nenhuma maneira.

Algumas empresas com mais topologias de rede complexo fazem a tradução de endereço de rede ou as conexões de proxy para o interior de suas redes. Nos casos, as perguntas de

SenderBase não trabalharão corretamente e devem ser desabilitadas no novo ouvinte. (do CLI, o **listenerconfig > edita > setup.**)

Se você tem alguma dúvida se os endereços estão sendo convertidos ou não ou se as conexões proxied, examine simplesmente o arquivo dos mail_logs (use um comando CLI tal como **mail_logs da cauda**). Isto mostra-lhe a cada conexão recebida a cada ouvinte, e poderá rapidamente ver se os endereços IP de Um ou Mais Servidores Cisco ICM NT que o ESA vê são dos Internet gerais ou não.

Nota: Seja cuidadoso olhar somente em conexões aos ouvintes públicos ou de entrada nos logs do correio ESA.

Informações Relacionadas

- [Cisco envia por correio eletrônico Guias do Usuário da ferramenta de segurança](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)