

Se um remetente negocia SMTPAUTH, que ajustes da política do CHAPÉU estão aplicados à sessão?

Índice

[Introdução](#)

[Solução](#)

Introdução

Este documento descreve como o S TP que retransmite (SMTPAUTH - autenticação S TP) pode ser introduz à ferramenta de segurança do email de Cisco (ESA).

Solução

Cisco envia por correio eletrônico ferramentas de segurança pode ser configurado para permitir que os remetentes autentiquem através de SMTPAUTH. SMTPAUTH não afeta ajustes da tabela do acesso host (CHAPÉU), remetentes está agrupado do “no grupo apropriado remetente” antes que a negociação SMTPAUTH comece. Quando um host de correio remoto conecta, o dispositivo primeiramente determinará que remetente o grupo aplica e impõe a política do correio para esse grupo do remetente. Por exemplo, se um MTA remoto “example.com” está em seu SUSPECTLIST Sendergroup, a política do REGULADOR DE PRESSÃO será aplicada, independentemente da negociação SMTPAUTH “example.com”.

Contudo, os remetentes que autenticam usando SMTPAUTH são tratados diferentemente dos remetentes “normais”. O comportamento da conexão para sessões bem sucedidas SMTPAUTH muda “PARA RETRANSMITIR,” eficazmente contornando “a tabela destinatária do acesso” (RATO) e LDAPACCEPT. Isto permite o remetente às mensagens de relé através do dispositivo da ferramenta de segurança do índice de Cisco. Como indicado, toda a taxa que limita ou que estrangula aquela aplica-se permanecerá de fato.