¿Si un remitente negocia SMTPAUTH, qué configuraciones de la directiva del SOMBRERO se aplican a la sesión?

Contenido

Introducción

Este documento describe cómo el S TP que retransmite (SMTPAUTH - autenticación S TP) puede ser introduce al dispositivo de seguridad del correo electrónico de Cisco (ESA).

Solución

Los dispositivos de seguridad del correo electrónico de Cisco se pueden configurar para permitir que los remitentes autentiquen vía SMTPAUTH. SMTPAUTH no afecta a las configuraciones de la tabla del acceso del host (SOMBRERO), los remitentes se agrupa en el “grupo apropiado del remitente” antes de que la negociación SMTPAUTH comience. Cuando un host de correo alejado conecta, la aplicación primero determinará que el grupo del remitente aplica e impone la directiva del correo para ese grupo del remitente. Por ejemplo, si un MTA del telecontrol “example.com” está en su SUSPECTLIST Sendergroup, la directiva de la VÁLVULA REGULADORA será aplicada, con independencia de la negociación SMTPAUTH “example.com”.

Sin embargo, tratan a los remitentes que autentican usando SMTPAUTH diferentemente de los remitentes “normales”. El comportamiento de la conexión para las sesiones acertadas SMTPAUTH cambia “PARA RETRANSMITIR,” con eficacia desviando la “tabla receptora del acceso” (RAT) y LDAPACCEPT. Esto permite el remitente a los mensajes de retransmisión a través del dispositivo del dispositivo de seguridad del contenido de Cisco. Según lo expuesto, seguirá habiendo cualquier tarifa que limita o que estrangula eso se aplica en efecto.