Si un expéditeur négocie SMTPAUTH, quels paramètres de la stratégie de CHAPEAU sont appliqués à la session ?

Contenu

Introduction

Ce document décrit comment le SMTP transmettant par relais (SMTPAUTH - authentification de SMTP) peut être introduisent à l'appliance de sécurité du courrier électronique de Cisco (ESA).

Solution

Des appliances de sécurité du courrier électronique de Cisco peuvent être configurées pour permettre à des expéditeurs pour authentifier par l'intermédiaire de SMTPAUTH. SMTPAUTH n'affecte pas des configurations de Tableau d'accès au hôte (CHAPEAU), des expéditeurs est groupé dans le « groupe d'expéditeur » approprié avant que la négociation SMTPAUTH commence. Quand un hôte de messagerie distant se connecte, l'appliance d'abord déterminera quel expéditeur le groupe applique et impose la stratégie de messagerie pour ce groupe d'expéditeur. Par exemple, si un distant MTA « example.com » est dans votre SUSPECTLIST Sendergroup, la stratégie de COMMANDE DE PUISSANCE sera appliquée, indépendamment de la négociation SMTPAUTH « example.com ».

Cependant, des expéditeurs qui authentifient utilisant SMTPAUTH sont traités différemment des expéditeurs « normaux ». Le comportement de connexion pour des sessions réussies SMTPAUTH change « POUR TRANSMETTRE PAR RELAIS, » efficacement sautant « le Tableau réceptif d'Access » (RAT) et LDAPACCEPT. Ceci permet l'expéditeur aux messages de relais par l'appliance d'appareils de sécurité du contenu de Cisco. Comme indiqué, n'importe quelle limitation de débit ou l'étranglement de cela s'applique restera en effet.