

如果发送方协商SMTPAUTH，什么帽子策略设置应用给会话？

目录

[简介](#)

[解决方案](#)

简介

本文描述中继的SMTP (SMTPAUTH - SMTP验证)如何可以是介绍到思科电子邮件安全工具(ESA)。

解决方案

思科电子邮件安全工具可以配置允许发送方通过SMTPAUTH验证。SMTPAUTH不影响主机访问表(帽子)设置，发送方分组到适合的“发送方组”，在SMTPAUTH协商开始前。当远程邮件主机连接，设备首先将确定哪发送方组应用并且强加该发送方组的邮件策略。例如，如果远程MTA “example.com”在您的SUSPECTLIST Sendergroup，节流孔策略将应用，不考虑“example.com”SMTPAUTH协商。

然而，验证使用SMTPAUTH的发送方对待与“正常”发送方不同。成功的SMTPAUTH会话的连接行为更改“中继”，有效绕过“接收访问表”(RATS)和LDAPACCEPT。这允许发送方对中转消息通过思科内容安全工具设备。如陈述，应用限制的任何的速率或限制将继续有效。