

送信者が SMTPAUTH をネゴシエートした場合、セッションにどの HAT ポリシー設定が適用されますか。

目次

[はじめに](#)

[解決策](#)

概要

中継で送る SMTP が Cisco E メール セキュリティ アプライアンス (ESA) に (SMTPAUTH - SMTP 認証) どのように導入するある場合もあるかこの資料に記述されています。

解決策

Cisco E メール セキュリティ アプライアンスは送信側を SMTPAUTH によって認証することを許可するために設定することができます。SMTPAUTH は適切な「送信側グループ」に SMTPAUTH ネゴシエーションが開始される前にホスト アクセス表 (帽子) 設定に、送信側グループ化されず影響を与えません。リモート メールホストが接続する場合、アプライアンスは最初にどの送信側をグループが加える判別し、その送信側グループかのためのメール ポリシーを課します。たとえば、リモート MTA が「SUSPECTLIST Sendergroup に example.com」あれば、スロットル ポリシーは「example.com」SMTPAUTH ネゴシエーションに関係なく適用します。

ただし、SMTPAUTH を使用して認証する送信側は「正常な」送信側と別様に扱われます。正常な SMTPAUTH セッションのための接続動作は中継で送るために「変化しま」効果的に「受信者のアクセス表」(RATS) および LDAPACCEPT をバイパスします。これは Cisco 内容セキュリティ アプライアンス モデル アプライアンスを通して中継通信文に送信側を可能にします。示されるように、それを制限するか、または絞るどのレートでも有効性を保ちます適用します。