

ASA ESMTP と SMTP の検査で Telnet 上の特定の コマンドが許可されない

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[問題](#)

[解決策](#)

[関連情報](#)

概要

このドキュメントでは、ASA を介して SMTP および ESMTP のトラフィックの接続の問題をトラブルシューティングする最適な方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco 5500 シリーズ適応型セキュリティ アプライアンス (ASA) に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

問題

ASA で Telnet によって E メール サーバをテストし、ESMTP または SMTP 検査を有効にしているとき、HELO や EHLO などの特定のコマンドで 550 エラーが返されます。このエラーは、コマンドが理解されないことを示します。ESMTP または SMTP 検査を無効にすると、コマンドは理解されず。

解決策

ESMTP および SMTP 検査では、特定のコマンドのみを ASA で許可するポリシーが実施されます。許可されていないメール コマンドを送信すると、そのコマンドは X で置き換えられ、そのコマンドはクライアントおよびサーバで無効となります。

一般的に許可されるコマンドは、『[Cisco ASA シリーズ コマンド リファレンス](#)』の「*inspect esmtp*」に記載されています。HELO と EHLO は一般的に許可されます。ただし、コマンドが認識されるかどうかは、テストの方法によって決まります。

たとえば、Telnet では各文字が別々のパケットで個別に送信されますが、実際の E メール クライアントおよびサーバでは、コマンド全体が 1 つのパケットで送信されます。Telnet を使用して「H」と入力すると、Telnet クライアントは「H」を E メール サーバに送信します。ESMTP および SMTP 検査では「H」が有効なコマンドとして認識されないため、ASA は「H」を「X」に置き換えて渡します。続けて「ELO」と入力すると、各文字は個別に送信され、ASA はそれぞれの文字を「X」に変えます。サーバは最終的なコマンドを「XXXX」として受信し、エラーを表示しますが、これは予想通りの結果です。

Telnet を使用して接続をテストする場合は、コマンド全体を 1 つのパケットで送信するようにアプリケーションを設定する必要があります (Microsoft Windows Telnet プログラムでは、1 文字ずつではなく、1 行ずつ送信できます)。CTRL+] を押して Telnet セッションを終了し、「send HELO」と入力してください。この操作により、文字ごとではなく、コマンド全体が送信されます。

代替策として、Netcat などの別のプログラムを使用できます。Netcat ではコマンドが 1 行ずつ送信されます。これは、ネットワーク ソケットとデータ転送をテストする強力なツールです。ただし、最適な解決策は、実際の E メール プログラムで接続をテストし、ASA でトラフィックを捕えてさらにテストすることです。

関連情報

- [テクニカルサポートとドキュメント - Cisco Systems](#)