EHLO の後に XXXXXXXA が表示され、STARTTLS の後に「500 #5.5.1 command not recognized」が表示されるのはなぜですか。

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス (ESA) に関連するメール サーバの通信および TLS の失敗で「XXXXXXXA」が表示される理由について説明します。

EHLO の後に XXXXXXXA が表示され、STARTTLS の後に「500 #5.5.1 command not recognized」が表示されるのはなぜですか。

TLS が、インバウンドまたはアウトバウンド メッセージで失敗します。

EHLO コマンドの後、ESA は外部メールサーバに対して次のように応答します。

```
250-8BITMIME\
250-SIZE 14680064
250 XXXXXXXA
```

SMTP メッセージ交換の「STARTTLS」コマンドの後、ESA は外部メールサーバに対して次のように応答します。

```
500 #5.5.1 command not recognized
```

STARTTLS の内部テストは成功しています。 つまり、ファイアウォールをバイパスするときに STARTTLS は問題なく機能しています (STARTTLS のローカル メール サーバとの接続や telnet インジェクション テストなど) 。

この問題は通常、Cisco PIX または Cisco ASA ファイアウォールを使用する場合に、SMTP パケット インスペクション (SMTP および ESMTP インスペクション、SMTP フィックスアップ プロトコル) と STARTTLS コマンドがファイアウォールで許可されなかったときに発生します。

各種の ESMTP セキュリティ プロトコルを使用する 7.2(3) よりも前のバージョンの Cisco PIX フ

ァイアウォールは、重複するヘッダーの解釈にバグがあるため、誤って接続を終了します。 ESMTP セキュリティ プロトコルには、「fixup」や「ESMTP inspect」などが含まれています。

PIX のすべての ESMTP セキュリティ機能をオフにするか、PIX を 7.2(3) 以降にアップグレードするか、またはその両方を行います。 この問題は、PIX が稼動するリモート電子メールの送信先で発生するため、この機能をオフにしたり、オフにすることを推奨したりするのは現実的でない場合があります。 推奨されていることを行う機会がある場合は、ファイアウォールのアップグレードによってこの問題が解決されるはずです。

問題の一部（全部ではない）は、他のヘッダーの内部にメッセージ ヘッダーが含まれている（特にドメイン キー（DK）および Domain Keys Identified Mail（DKIM）の署名ヘッダー）ために発生します。 PIX が誤って SMTP セッションを終了することで配信が失敗する状況は他にもありますが、DK および DKIM の署名が既知の原因の 1 つです。 DK または DKIM を一時的に無効にすれば、この問題をとりあえず解決できますが、最善の解決策は、すべての PIX ユーザがこれらのセキュリティ機能をアップグレードまたは無効化することです。

すべてのユーザが引き続き DKIM を使ってメッセージに署名し、この機能をまだ使用していない場合はその使用を検討することを推奨します。

SMTP および ESMTP インスペクション（PIX/ASA 7.x 以降）については、次を参照してください。

/c/en/us/support/docs/security/pix-500-series-security-appliances/69374-pix7x-mailserver.html

ESMTP TLS の設定：

```
pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(config-pmap)#exit
```

SMTP

http://www.cisco.com/en/US/docs/security/pix/pix62/configuration/guide/fixup.html

show fixup コマンドを使用して、フィックスアップ プロトコルの明示的な（設定可能な）設定を表示できます。 設定可能なプロトコルのデフォルト設定は次のとおりです。

```
show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
```

関連情報

- AsyncOS for Email ユーザ ガイド
- GLO サポート連絡先情報

- テクニカル サポートとドキュメント – Cisco Systems