

# Pourquoi voyez-vous après la commande EHLO et "500 #5.5.1 non identifiée » après STARTTLS ?

## Contenu

[Introduction](#)

[Pourquoi voyez-vous après la commande EHLO et "500 #5.5.1 non identifiée » après STARTTLS ?](#)

[Informations connexes](#)

## Introduction

Ce document décrit pourquoi vous voyez « » dans la transmission de mail server et les pannes de TLS associées avec l'appliance de sécurité du courrier électronique de Cisco (ESA).

## Pourquoi voyez-vous après la commande EHLO et "500 #5.5.1 non identifiée » après STARTTLS ?

Le TLS échoue pour les messages d'arrivée ou sortants.

Après la commande EHLO, l'ESA répond à un mail server externe avec :

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

Après la commande « STARTTLS » dans la conversation de SMTP, l'ESA répond à un mail server externe avec :

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

Les tests internes pour STARTTLS sont réussis. Cela signifie en sautant le Pare-feu, STARTTLS fonctionne bien, comme des connexions STARTTLS avec les serveurs de messagerie ou les tests locaux d'injection de telnet.

Le problème est typiquement vu quand vous utilisez un Pare-feu de Cisco Pix ou de Cisco ASA quand inspection de SMTP et ESMTP d'inspection de paquet de SMTP (, SMTP Fixup Protocol) et on ne permet pas la commande STARTTLS dans le Pare-feu.

Les versions de Pare-feu de Cisco PIX plus tôt que 7.2(3) qui les utilisent les divers protocoles de Sécurité ESMTP terminent inexactement des connexions en raison d'une bogue en interprétant les en-têtes en double. Les protocoles de Sécurité ESMTP incluent le « fixup, » « ESMTP

examenent, » et d'autres.

Arrêtez toutes les fonctionnalités de sécurité ESMTP dans PIX, ou améliorez PIX à 7.2(3) ou plus tard, ou chacun des deux. Puisque ce problème se pose avec les destinations distantes d'email que le passage PIX, il ne pourrait pas être pratique pour arrêter ceci ou pour recommander l'arrêter. Si vous avez l'occasion d'émettre une recommandation, une mise à jour de Pare-feu devrait résoudre ce problème.

Certains, pas toutes les, questions sont dus à l'intégration des en-têtes de message dans d'autres en-têtes, notamment les en-têtes de signature pour les clés de domaine et la messagerie identifiée par clés de domaine. Tandis qu'il restent d'autres circonstances sous lesquelles PIX termine inexactement une session de SMTP et entraîne des pannes de la livraison, la signature du DK et DKIM est une cause connue. Désactiver temporairement le DK ou DKIM pourrait résoudre ce problème pour l'instant, mais la meilleure solution est pour que tous les utilisateurs PIX améliorent ou pour désactivent ces fonctionnalités de sécurité.

Cisco recommande que tous les clients continuent à signer des messages avec DKIM et à envisager d'utiliser cette caractéristique sinon faisant déjà ainsi.

Pour l'inspection de SMTP et ESMTP (PIX/ASA 7.x et ci-dessus) voyez s'il vous plaît :

[/c/en/us/support/docs/security/pix-500-series-security-appliances/69374-pix7x-mailserver.html](http://c/en/us/support/docs/security/pix-500-series-security-appliances/69374-pix7x-mailserver.html)

Configuration de TLS ESMTP :

```
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
```

Pour le SMTP Fixup Protocol veuillez voir :

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

Vous pouvez visualiser les configurations (configurables) explicites de protocole de fixup avec la commande de fixup d'exposition. Les valeurs par défaut pour des protocoles configurables sont comme suit :

```
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
```

## **[Informations connexes](#)**

- [Guide utilisateur d'email d'AsyncOS](#)
- [L'information de contact de support GLO](#)
- [Support et documentation techniques - Cisco Systems](#)