

¿Por qué usted ve después de EHLO y el comando "500 #5.5.1 no reconocido" después de STARTTLS?

Contenido

[Introducción](#)

[¿Por qué usted ve después de EHLO y el comando "500 #5.5.1 no reconocido" después de STARTTLS?](#)

[Información Relacionada](#)

Introducción

Este documento describe porqué usted ve que "" en la comunicación del mail server y errores de TLS asociados a Cisco envían por correo electrónico el dispositivo de seguridad (ESA).

¿Por qué usted ve después de EHLO y el comando "500 #5.5.1 no reconocido" después de STARTTLS?

TLS falla para entrante o los mensajes de salida.

Después del comando EHLO, el ESA responde a un mail server externo con:

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

Después del comando "STARTTLS" en la conversación SMTP, el ESA responde a un mail server externo con:

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

Las pruebas internas para STARTTLS son acertadas. Eso significa al desviar el Firewall, los trabajos STARTTLS muy bien, por ejemplo las conexiones STARTTLS con los servidores del correo o las pruebas locales de la inyección telnet.

El problema se considera típicamente cuando usted utiliza un Firewall de Cisco Pix o de Cisco ASA cuando examen del paquete SMTP (S TP y La inspección ESMTP, fixup protocol S TP) y el comando STARTTLS no se permite en el Firewall.

Las versiones del Cisco PIX Firewall de 7.2(3) que utilizan los diversos protocolos de Seguridad ESMTP terminan anterior incorrectamente las conexiones debido a un bug en la interpretación de las encabezados duplicados. Los protocolos de Seguridad ESMTP incluyen el "fixup," "ESMTP

examinan,” y otros.

Apague todas las funciones de seguridad ESMTP en el PIX, o actualice el PIX a 7.2(3) o más adelante, o ambos. Puesto que este problema ocurre con los destinos remotos del correo electrónico que ejecutan el PIX, puede ser que no sea práctico apagar esto o recomendarlo el apagar de él. Si usted tiene la oportunidad de hacer una recomendación, una actualización del Firewall debe solucionar este problema.

Algunos, no todos los, problemas son debido a la inclusión de los encabezados del mensaje dentro de otras encabezados, notablemente las encabezados de la firma para las claves del dominio y el correo identificado las claves del dominio. Mientras que todavía hay otras circunstancias bajo las cuales el PIX termina incorrectamente a una sesión de SMTP y causa los errores de la salida, la firma DK y DKIM es una causa sabida. Temporalmente inhabilitar DK o el DKIM pudo solucionar este problema de momento, pero la mejor solución está para que todos los usuarios PIX actualicen o inhabiliten estas funciones de seguridad.

Cisco recomienda que todos los clientes continúan firmando los mensajes con el DKIM y considerándolos usar esta característica si no que hace ya tan.

Para S TP y el La inspección ESMTP (PIX/ASA 7.x y arriba) vea por favor:

[/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)

Configuración ESMTP TLS:

```
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
```

Para el fixup protocol S TP satisfaga ven:

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

Usted puede ver las configuraciones (configurables) explícitas del fixup protocol con el comando fixup de la demostración. Las configuraciones predeterminadas para los protocolos configurables son como sigue:

```
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
```

Información Relacionada

- [Guía del usuario del correo electrónico de AsyncOS](#)
- [Información de contacto del soporte GLO](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)