Por que você vê após o comando EHLO e "500 #5.5.1 não reconhecido” após STARTTLS?

Índice

Introdução

Este documento descreve porque você vê que “” em uma comunicação do mail server e nas falhas TLS associadas com Cisco enviam por correio eletrónico a ferramenta de segurança (ESA).

Por que você vê após o comando EHLO e "500 #5.5.1 não reconhecido” após STARTTLS?

O TLS falha para de entrada ou mensagens externa.

Após o comando EHLO, o ESA responde a um mail server externo com:

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

Após o comando “STARTTLS” na conversação SMTP, o ESA responde a um mail server externo com:

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

Os testes internos para STARTTLS são bem sucedidos. Isso significa ao contornear o Firewall, trabalhos STARTTLS muito bem, como conexões STARTTLS com os server do correio ou os testes locais da injeção do telnet.

O problema é considerado tipicamente quando você usa um Firewall de Cisco Pix ou de Cisco ASA quando inspeção do pacote SMTP (S TP e inspeção de ESMTP, fixup protocol S TP) e o comando STARTTLS não é permitido no Firewall.

As versões do Cisco PIX Firewall mais cedo de 7.2(3) que se usam os vários protocolos de segurança ESMTP terminam incorretamente conexões devido a um erro em interpretar encabeçamentos duplicados. Os protocolos de segurança ESMTP incluem “reparares,” “ESMTP inspecionam,” e outro.

Desligue todos os recursos de segurança ESMTP no PIX, ou promova o PIX a 7.2(3) ou mais atrasado, ou ambos. Desde que este problema ocorre com os destinos remotos do email que executam o PIX, não pôde ser prático desligar este ou recomendá-lo desligá-lo. Se você tem a oportunidade de fazer uma recomendação, uma elevação do Firewall deve resolver esta edição.

Alguns, não todas as, edições são devido à inclusão dos cabeçalhos da mensagem dentro de outros encabeçamentos, notavelmente os encabeçamentos da assinatura para chaves do domínio e o correio identificado chaves do domínio. Quando houver ainda outras circunstâncias sob que o PIX termina incorretamente uma sessão de SMTP e causa falhas da entrega, a assinatura DK e DKIM é uma causa conhecida. Temporariamente desabilitar DK ou DKIM pôde resolver esta edição pelo momento, mas a melhor solução é para que todos os usuários PIX promovam ou desabilitem estes recursos de segurança.

Cisco recomenda que todos os clientes continuam a assinar mensagens com DKIM e às considerar usar esta característica se não já que faz assim.

Para S TP e inspeção de ESMTP (PIX/ASA 7.x e acima) veja por favor:

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

Configuração 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 o fixup protocol S TP veja por favor:

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

Você pode ver os ajustes (configuráveis) explícitos do fixup protocol com o comando fixup da mostra. As configurações padrão para protocolos configuráveis são como segue:

```
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
```

Informações Relacionadas

- Guia do Usuário do email de AsyncOS
- Informação de contato do apoio GLO
- Suporte Técnico e Documentação - Cisco Systems