Perché viene visualizzato XXXXXXXA dopo EHLO e "500 #5.5.1 command not recognition" dopo STARTTLS?

Sommario

Introduzione

Questo documento descrive il motivo per cui "XXXXXXA" viene visualizzato nelle comunicazioni tra server di posta e negli errori TLS associati a Cisco Email Security Appliance (ESA).

Perché viene visualizzato XXXXXXXA dopo EHLO e "500 #5.5.1 command not recognition" dopo STARTTLS?

TLS non riuscito per i messaggi in entrata o in uscita.

Dopo il comando EHLO, l'ESA risponde a un server di posta esterno con:

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

Dopo il comando "STARTTLS" nella conversazione SMTP, l'ESA risponde a un server di posta esterno con:

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

I test interni per STARTTLS sono stati completati. Ciò significa che quando si ignora il firewall, STARTTLS funziona correttamente, come le connessioni STARTTLS con i server di posta locali o i test di inserimento telnet.

Il problema si verifica in genere quando si utilizza un firewall Cisco Pix o Cisco ASA con il comando SMTP Packet Inspection (SMTP e ESMTP Inspection, SMTP Fixup Protocol) e il comando STARTTLS non è consentito nel firewall.

Le versioni di Cisco PIX firewall precedenti alla 7.2(3) che utilizzano i vari protocolli di sicurezza ESMTP terminano le connessioni in modo errato a causa di un bug nell'interpretazione delle intestazioni duplicate. I protocolli di sicurezza ESMTP includono "correzione", "ESMTP inspect" e

altri.

Disattivare tutte le funzioni di sicurezza ESMTP in PIX, aggiornare PIX a 7.2(3) o versioni successive o entrambe. Poiché questo problema si verifica con le destinazioni di posta elettronica remote che eseguono PIX, potrebbe non essere pratico disattivarlo o consigliarlo. Se si ha la possibilità di formulare un suggerimento, un aggiornamento del firewall dovrebbe risolvere questo problema.

Alcuni problemi, non tutti, sono dovuti all'inclusione delle intestazioni dei messaggi in altre intestazioni, in particolare le intestazioni delle firme per le chiavi di dominio e i messaggi identificati con le chiavi di dominio. Anche se ci sono ancora altre circostanze in cui PIX termina in modo errato una sessione SMTP e causa errori di recapito, la firma DK e DKIM è una causa nota. La disattivazione temporanea di DK o DKIM potrebbe risolvere il problema per il momento, ma la soluzione migliore è che tutti gli utenti PIX aggiornino o disattivino queste funzioni di sicurezza.

Cisco consiglia a tutti i clienti di continuare a firmare i messaggi con DKIM e di considerare l'opportunità di utilizzare questa funzione, se non lo fanno già.

Per l'ispezione SMTP ed ESMTP (PIX/ASA 7.x e versioni successive), vedere:

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

Configurazione 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
```

Per il protocollo di correzione SMTP, vedere:

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

Per visualizzare le impostazioni esplicite (configurabili) del protocollo di correzione, usare il comando show fixup. Le impostazioni predefinite per i protocolli configurabili sono le seguenti:

```
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
```

Informazioni correlate

- Guida per l'utente di AsyncOS Email
- Informazioni di contatto del supporto GLO
- Documentazione e supporto tecnico – Cisco Systems