Waarom ziet u XXXXXA na EHLO en de "500 #5.5.1 opdracht niet herkend" na STARTTLS?

Inhoud

Inleiding

Dit document beschrijft waarom u "XXXXXXXA" ziet in communicatie met mailservers en TLS-fouten die bij de Cisco e-mail security applicatie (ESA) zijn gekoppeld.

Waarom ziet u XXXXXA na EHLO en de "500 #5.5.1 opdracht niet herkend" na STARTTLS?

TLS faalt voor inkomende of uitgaande berichten.

Na de EHLO-opdracht reageert de ESA op een externe mailserver met:

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

Na opdracht "STARTTLS" in de discussie in TCP reageert de ESA op een externe mailserver met:

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

Interne tests voor STARTTLS zijn succesvol. Dat betekent dat wanneer u de firewall omzeilt, STARTTLS goed werkt, zoals STARTTLS-verbindingen met de lokale mailservers of telnet-injectietests.

Het probleem wordt normaal gezien wanneer u een Cisco Pix of Cisco ASA firewall gebruikt wanneer MGTP-pakketinspectie (mtp- en ESMTP-inspectie, mtp-protocol) en de opdracht STARTTLS niet in de firewall is toegestaan.

Cisco PIX-firewallversies eerder dan 7.2(3) die de verschillende ESMTP-beveiligingsprotocollen onjuist gebruiken om verbindingen te beëindigen vanwege een bug in het interpreteren van dubbele headers. De ESMTP veiligheidsprotocollen omvatten "fixup," "ESMTP inspectie," en anderen.

Schakel alle ESMTP-beveiligingsfuncties in PIX uit, of upgrade PIX naar 7.2(3) of hoger, of beide. Aangezien dit probleem zich voordoet met afgelegen e-mailbestemmingen die PIX uitvoeren, is

het mogelijk dat dit niet praktisch is om dit uit te schakelen of om dit aan te raden. Als u de mogelijkheid hebt om een aanbeveling te maken, zou een firewallupgrade dit probleem moeten oplossen.

Sommige, niet alle, problemen zijn het gevolg van het opnemen van berichtkopregels in andere kopregels, in het bijzonder de kenmerkende kopregels voor Domain Keys en Domain Keys Identified Mail. Hoewel er nog andere omstandigheden zijn waaronder PIX een sessie onjuist beëindigt en leveringsfouten veroorzaakt, is het ondertekenen van DK en DKIM een bekende oorzaak. Tijdelijk uitschakelen van DK of DKIM kan dit probleem voorlopig oplossen, maar de beste oplossing is voor alle PIX-gebruikers om deze beveiligingsfuncties te verbeteren of uit te schakelen.

Cisco raadt aan dat alle klanten berichten met DKIM blijven ondertekenen en om te overwegen deze optie te gebruiken als u dit al doet.

Voor MTP- en ESMTP-inspectie (PIX/ASA 7.x en hoger) zie:

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

ESMTP-TLS-configuratie:

```
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
```

Zie voor het protocol voor het opslaan van MTP-bestanden:

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

U kunt de expliciete (configureerbare) protocolinstellingen bekijken met de opdracht voor het maken van een show. De standaardinstellingen voor configureerbare protocollen zijn als volgt:

```
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
```

Gerelateerde informatie

- Gebruikershandleiding AsyncOS
- Contactinformatie voor GLO-ondersteuning
- Technische ondersteuning en documentatie – Cisco Systems