Warum sehen Sie XXXXXXXA nach EHLO und "500 #5.5.1 Befehl nicht erkannt" nach STARTTLS?

Inhalt

Einführung

In diesem Dokument wird erläutert, warum Sie "XXXXXXXA" bei der Kommunikation mit dem Mailserver und bei TLS-Fehlern sehen, die mit der Cisco E-Mail Security Appliance (ESA) verbunden sind.

Warum sehen Sie XXXXXXXA nach EHLO und "500 #5.5.1 Befehl nicht erkannt" nach STARTTLS?

TLS schlägt bei ein- oder ausgehenden Nachrichten fehl.

Nach dem EHLO-Befehl antwortet die ESA auf einen externen Mailserver mit:

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

Nach dem Befehl "STARTTLS" in der SMTP-Konversation antwortet die ESA auf einen externen Mailserver mit:

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

Die internen Tests für STARTTLS sind erfolgreich. Das bedeutet, dass STARTTLS bei Umgehung der Firewall einwandfrei funktioniert, z. B. STARTTLS-Verbindungen mit den lokalen Mail-Servern oder Telnet-Injektionstests.

Das Problem tritt in der Regel dann auf, wenn Sie eine Cisco Pix- oder Cisco ASA-Firewall verwenden, wenn SMTP Packet Inspection (SMTP und ESMTP Inspection, SMTP Fixup Protocol) und der STARTTLS-Befehl in der Firewall nicht zulässig sind.

Cisco PIX-Firewall-Versionen vor 7.2(3), die die verschiedenen ESMTP-Sicherheitsprotokolle verwenden, beenden Verbindungen aufgrund eines Fehlers bei der Interpretation doppelter

Header falsch. Zu den ESMTP-Sicherheitsprotokollen gehören "fixup", "ESMTP inspect" und andere.

Deaktivieren Sie alle ESMTP-Sicherheitsfunktionen in PIX, oder aktualisieren Sie PIX auf 7.2(3) oder höher oder beides. Da dieses Problem bei Remote-E-Mail-Zielen auftritt, auf denen PIX ausgeführt wird, ist es möglicherweise nicht sinnvoll, diese Funktion zu deaktivieren oder sie zu deaktivieren. Wenn Sie die Möglichkeit haben, eine Empfehlung abzugeben, sollte dieses Problem durch ein Firewall-Upgrade gelöst werden.

Einige, nicht alle der Probleme sind auf die Einbeziehung von Nachrichtenheadern in andere Header, insbesondere die Signatur-Header für Domain Keys und Domain Keys Identified Mail. Während es noch andere Umstände gibt, unter denen PIX eine SMTP-Sitzung fälschlicherweise beendet und Lieferfehler verursacht, ist die Signierung von DK und DKIM eine bekannte Ursache. Die vorübergehende Deaktivierung von DK oder DKIM könnte dieses Problem vorerst beheben, aber die beste Lösung ist für alle PIX-Benutzer, diese Sicherheitsfunktionen zu aktualisieren oder zu deaktivieren.

Cisco empfiehlt, dass alle Kunden weiterhin Nachrichten mit DKIM unterzeichnen und, falls nicht bereits vorhanden, die Verwendung dieser Funktion in Erwägung ziehen.

Informationen zur SMTP- und ESMTP-Prüfung (PIX/ASA 7.x und höher) finden Sie unter:

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

ESMTP TLS-Konfiguration:

```
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
```

Informationen zum SMTP-Fixup-Protokoll finden Sie unter:

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

Sie können die expliziten (konfigurierbaren) Fixup-Protokoll-Einstellungen mit dem Befehl show fixup anzeigen. Die Standardeinstellungen für konfigurierbare Protokolle sind wie folgt:

```
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
```

Zugehörige Informationen

- AsyncOS E-Mail-Benutzerhandbuch
- Kontaktdaten des GLO-Supports
- Technischer Support und Dokumentation - Cisco Systems