Fehlerbehebung bei periodischen Problemen und unterbrochenen Verbindungen während des Empfangs und Zustellens von E-Mails

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie gelegentliche Probleme und abgebrochene Verbindungen während des Empfangs und der Zustellung von E-Mails behoben werden.

Voraussetzungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Private Internet eXchange (PIX) oder Adaptive Security Appliance (ASA) ab Version 7.x
- Cisco E-Mail Security Appliance (ESA)

Hintergrundinformationen

Die Cisco ESA E-Mail-Gateways sind per E-Mail verwaltete Firewalls. Somit ist keine Upstream-Firewall wie Cisco PIX oder ASA erforderlich, um den E-Mail-Verkehr von und zu einer ESA zu überprüfen. Es wird empfohlen, die ESMTP-Anwendungsinspektionsfunktionen (Extended Simple Mail Transfer Protocol) auf der Firewall für alle Host-Adressen der Sicherheits-Appliance zu deaktivieren. Die ESMTP-Protokollüberprüfung ist standardmäßig für alle Verbindungen aktiviert, die die Cisco Firewalls durchlaufen. Dies bedeutet, dass alle Befehle, die zwischen Mail-Gateways über TCP-Port 25 sowie zwischen einzelnen Nachrichten-Headern ausgegeben werden, analysiert werden, um strikt den Request for Comments (RFC)-Spezifikationen zu entsprechen, die die RFC 821, 1123 und 1870 enthalten. Es gibt definierte Standardwerte für die maximale Anzahl von Empfängern und Nachrichtengrößen, die Probleme bei der Zustellung an und von der ESA

verursachen können. Diese speziellen Konfigurationsstandardwerte sind hier aufgeführt (entnommen vom Cisco Command Lookup Tool).

Der Befehl **inspect esmtp** umfasst die Funktionalität, die zuvor durch den Befehl **fixup smtp** bereitgestellt wurde, und bietet zusätzliche Unterstützung für einige ESMTP-Befehle. Die ESMTP-Anwendungsinspektion bietet Unterstützung für acht ESMTP-Befehle, einschließlich AUTH, EHLO, ETRN, HELP, SAML, SEND, **SOML** und **VRFY.** Neben der Unterstützung von sieben RFC 821-Befehlen (**DATA**, **HELO**, **MAIL**, **NOOP**, **QUIT, RCPT, RSET) unterstützt die Sicherheits-Appliance insgesamt 15 SMTP-Befehle.** Andere ESMTP-Befehle wie **ATRN**, **STARTLS**, **ONEX**, **VERB**, **CHUNKING und private Erweiterungen werden nicht unterstützt.** Nicht unterstützte Befehle werden in Xs übersetzt, die vom internen Server abgelehnt werden. Dies führt zu einer Meldung wie **500 Command unbekannt: XXX**. Unvollständige Befehle werden verworfen.

Der Befehl **inspect esmtp** ändert die Zeichen im SMTP-Server-Banner in Sternchen außer den Zeichen "2", "0" und "0". Zeichen zur Wagenrückgabe (CR) und Zeilenvorschub (LF) werden ignoriert. Bei aktivierter SMTP-Überprüfung wartet eine Sitzung für interaktives SMTP auf einen gültigen Befehl, und der Firewall-Server "esmtp state" behält die korrekten Zustände für die Sitzung bei, wenn diese Regeln nicht eingehalten werden:

- SMTP-Befehle müssen mindestens vier Zeichen lang sein.
- SMTP-Befehle müssen mit Wagenrücklauf und Zeilenvorschub beendet werden.
- SMTP-Befehle müssen auf eine Antwort warten, bevor die nächste Antwort ausgegeben wird.

Ein SMTP-Server antwortet auf Client-Anfragen mit numerischen Antwortcodes und optionalen, für Menschen lesbaren Zeichenfolgen. SMTP-Anwendungsinspektion kontrolliert und reduziert die Befehle, die der Benutzer verwenden kann, sowie die vom Server zurückgegebenen Meldungen. Die SMTP-Prüfung führt drei Hauptaufgaben aus:

- Beschränkt SMTP-Anforderungen auf sieben grundlegende SMTP-Befehle und acht erweiterte Befehle.
- Überwacht die SMTP-Befehls-Antwortsequenz.
- Generiert einen Prüfpfad. Der Audit-Datensatz 108002 wird generiert, wenn ein ungültiges Zeichen, das in die E-Mail-Adresse eingebettet ist, ersetzt wird. Weitere Informationen finden Sie unter RFC 821.

Eine SMTP-Prüfung überwacht die Befehls- und Antwortsequenz für die folgenden ungewöhnlichen Signaturen:

- Abgeschnittene Befehle.
- Falsche Befehlsbeendigung (nicht terminiert mit <CR><LR>).
- Wenn die PHY Interface for PCI Express (PIPE)-Signatur als Parameter für eine **MAIL** von oder **RCPT** zu Befehlen gefunden wird, wird die Sitzung geschlossen. Er kann vom Benutzer nicht konfiguriert werden.
- Unvorhergesehener Übergang durch den SMTP-Server.
- Bei unbekannten Befehlen ändert die Sicherheits-Appliance alle Zeichen im Paket in **X**. In diesem Fall generiert der Server einen Fehlercode für den Client. Aufgrund der Paketänderung muss die TCP-Prüfsumme neu berechnet oder angepasst werden.
- Bearbeitung von TCP-Streams

Die Ausgabe von **show service policy inspect ESMTP** enthält die Standardüberprüfungswerte und die entsprechenden Aktionen.

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Problem

Gelegentlich werden Nachrichten nicht korrekt von der Cisco ESA geliefert oder empfangen. Eine oder mehrere dieser Meldungen werden im E-Mail-Protokoll des Cisco ESA-Geräts angezeigt:

- Nachricht abgebrochen MID XXX
- Erhalt abgebrochener ICID 21916 verloren
- ICID 21916 Schließen
- Verbindungsfehler: DCID: XXX-Domäne:example.com IP: 10.1.2.3-Port: 25 Details: [Fehler 60]
  Zeitüberschreitungsschnittstelle für Betrieb: 10.10.10.1 Grund: Netzwerkfehler

Lösung

Einige dieser Standardeinstellungen können sich auf die Bereitstellung verschlüsselter TLS-Nachrichten (Transport Layer Security), Mailinglistenkampagnen und die Fehlerbehebung auswirken. Bei einer besseren Richtlinie können Sie die Firewall verwenden, um den gesamten verbleibenden E-Mail-Datenverkehr zu überprüfen, der nicht zuerst über die Sicherheits-Appliance geleitet wird, und dabei den gesamten Datenverkehr auszunehmen, der vorhanden ist. In diesem Beispiel wird veranschaulicht, wie die Standardkonfiguration (siehe oben) so angepasst wird, dass die ESMTP-Anwendungsinspektion für eine einzelne Sicherheits-Host-Adresse ausgenommen wird.

Sie können den gesamten Datenverkehr zu und von der internen Adresse der Cisco ESAs als Referenz in einer MPF-Klassenzuordnung (Modular Policy Framework) definieren:

```
access-list ironport_esa_internal extended permit ip any 192.168.1.1
access-list ironport_esa_internal extended permit ip 192.168.1.1 any
```

Dadurch wird eine neue Klassenzuordnung erstellt, die Datenverkehr gezielt abgleicht oder anders behandelt werden soll:

```
class-map ironport_esa
match address ironport_esa_internal
```

In diesem Abschnitt wird die neue Cisco Klassenzuordnung verknüpft und die ESMTP-Protokollprüfungsfunktionen deaktiviert:

```
policy-map global_policy
class ironport_esa
no inspect esmtp
```

Beachten Sie auch die Anweisung für die Adressübersetzung, mit der die Anzahl der eingehenden und halb offenen (embryonalen) Verbindungen an die Adresse gesteuert werden kann. Dies ist nützlich, um Denial-of-Service-Angriffe (DoS) zu bekämpfen, kann jedoch Lieferraten beeinträchtigen.

Format zum Nachverfolgen von Parametern von **NAT-** und **STATIC-**Befehlen ... [tcp (max_conns)] [max_embryonal].
In diesem Beispiel werden die Grenzen von 50 TCP-Verbindungen insgesamt und 100 halb offenen oder embryonalen Verbindungsversuchen festgelegt:

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```