

Was bedeuten "Empfang abgebrochen" und "Empfang abgebrochen von Absender" in den Mail-Protokollen?

Inhalt

[Einführung](#)

[Was bedeutet "Empfang abgebrochen" in den Mail-Protokollen?](#)

[Was bedeutet "Empfang abgebrochen durch Absender" in den Mail-Protokollen?](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird der Unterschied zwischen "Empfangen abgebrochen" und "Empfangen abgebrochen durch Absender" beschrieben, wie in den E-Mail-Protokollen und der Nachrichtenverfolgung im Zusammenhang mit der Cisco Email Security Appliance (ESA) und der Cisco Security Management Appliance (SMA) zu sehen ist.

Was bedeutet "Empfang abgebrochen" in den Mail-Protokollen?

"MID XXX Receiving aborted" gibt an, dass die Verbindung von der Empfängerseite durch ein Netzwerkproblem beendet wurde oder der Absender die Verbindung einfach abrupt geschlossen hat. "MID XXX" ist die Nachrichten-ID der Nachricht, die nicht erfolgreich injiziert werden konnte. In vielen Fällen, in denen "Empfang abgebrochen" zu sehen ist, wird der Datenverkehr durch eine Firewall oder ein SMTP-fähiges Sicherheitsgerät unterbrochen.

Im folgenden Beispiel wird ein Remote-Client veranschaulicht, der eine SMTP-Verbindung zur ESA herstellt, gefolgt von der Verbindung, die unter der Anwendungsschicht geschlossen wird. Dies wird in der Regel beobachtet, wenn die Appliance ein vorzeitiges TCP [FIN]-Flag oder einen Verbindungsrücksetzvorgang empfängt.

```
Thu Aug 14 11:04:31 2014 Info: New SMTP ICID 10293 interface Management
(192.168.0.199) address 192.168.0.200 reverse dns host ns.example.com verified no
Thu Aug 14 11:04:31 2014 Info: ICID 10293 RELAY SG RELAY_SG match 192.168.0.200
SBRS not enabled
Thu Aug 14 11:04:51 2014 Info: Start MID 1404 ICID 10293
Thu Aug 14 11:04:51 2014 Info: MID 1404 ICID 10293 From: <user@domain.com>
Thu Aug 14 11:05:00 2014 Info: MID 1404 ICID 10293 RID 0 To: <end_user@example.com>
Thu Aug 14 11:05:36 2014 Info: ICID 10293 lost
Thu Aug 14 11:05:36 2014 Info: Message aborted MID 1404 Receiving aborted
Thu Aug 14 11:05:36 2014 Info: Message finished MID 1404 aborted
Thu Aug 14 11:05:36 2014 Info: ICID 10293 close
```

Dies kann auch einfach bedeuten, dass das für den Listener konfigurierte Timeout für nicht erfolgreiche eingehende Verbindungen erreicht wurde (standardmäßig fünf Minuten). Dies tritt auf, wenn vor Erreichen des Timeouts keine Daten gesendet wurden:

```
Wed Aug 20 22:20:07 2014 Info: Start MID 1558778 ICID 3875465
Wed Aug 20 22:20:07 2014 Info: MID 1558778 ICID 3875465 From: <sndr@xyz.com>
Wed Aug 20 22:20:07 2014 Info: MID 1558778 ICID 3875465 RID 0 To:
```

```
Wed Aug 20 22:25:07 2014 Info: Message aborted MID 1558778 Receiving aborted
Wed Aug 20 22:25:07 2014 Info: Message finished MID 1558778 aborted
```

Was bedeutet "Empfang abgebrochen durch Absender" in den Mail-Protokollen?

"MID XXX Receiving aborted by sender" gibt an, dass es die Absenderseite ist, die vor "data" ein "quit" gesendet hat, um eine SMTP-Unterhaltung zu beenden. "MID XXX" ist die Nachrichten-ID der Nachricht, die nicht erfolgreich injiziert werden konnte.

Im folgenden Beispiel wird ein Remote-Client veranschaulicht, der eine SMTP-Verbindung zur ESA herstellt, gefolgt von der Clientseite, die die Verbindung auf der Anwendungsebene mit dem SMTP-Befehl "quit" schließt:

```
Thu Aug 14 13:08:49 2014 Info: New SMTP ICID 10318 interface Management
(192.168.0.199) address 192.168.0.200 reverse dns host ns.example.com verified no
Thu Aug 14 13:08:49 2014 Info: ICID 10318 RELAY SG RELAY_SG match 192.168.0.200
SBRS not enabled
Thu Aug 14 13:08:56 2014 Info: Start MID 1412 ICID 10318
Thu Aug 14 13:08:56 2014 Info: MID 1412 ICID 10318 From: <user@domain.com>
Thu Aug 14 13:09:03 2014 Info: MID 1412 ICID 10318 RID 0 To: <end_user@example.com>
Thu Aug 14 13:09:06 2014 Info: Message aborted MID 1412 Receiving aborted by sender
Thu Aug 14 13:09:06 2014 Info: Message finished MID 1412 aborted
Thu Aug 14 13:09:06 2014 Info: ICID 10318 close
```

Fehlerbehebung

- Richten Sie für weitere Untersuchungen Debug-Protokolle für die Injektion für den Mail-Server der betreffenden Partnerdomäne ein. Injektion-Debug-Protokolle zeigen Ihnen genau, was Sie von diesem Host zur Appliance erhalten.

Hinweis: Sie müssen möglicherweise Debug-Protokolle für die Injektion für jeden Mail-Host konfigurieren, der in den DNS-MX-Datensätzen des Partners aufgeführt ist.

- Möglicherweise ist es auch sinnvoll, während der Kommunikation eine Paketerfassung auf der Appliance auszuführen, um die vollständige Verbindung und den Handshake sowie die damit verbundenen Probleme anzuzeigen, die möglicherweise zu einer Unterbrechung der Verbindung führen.

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Was ist eine Nachrichten-ID \(MID\), eine Injection Connection ID \(ICID\) oder eine Delivery Connection ID \(DCID\)?](#)
- [Wie analysieren Sie zeitweilige E-Mail-Zustellungsprobleme auf der ESA?](#)
- [ESA-Paketerfassungsverfahren](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)