

Wie kann ich eine Fehlerbehebung durchführen, wenn das Cisco Secure Email Gateway keine Nachricht empfangen hat?

Inhalt

[Einführung](#)

[Wie kann ich eine Fehlerbehebung durchführen, wenn das Cisco Secure Email Gateway keine Nachricht empfangen hat?](#)

Einführung

In diesem Dokument wird beschrieben, warum das Cisco Secure Email Gateway keine Nachricht erhält, sowie Optionen zur Problembeseitigung.

Wie kann ich eine Fehlerbehebung durchführen, wenn das Cisco Secure Email Gateway keine Nachricht empfangen hat?

Um eine Fehlerbehebung beim Empfang von Nachrichten durchzuführen, müssen Sie die IP-Adressen kennen, die zum Senden von E-Mails durch die Organisation verwendet wurden, die die E-Mail gesendet hat. In der Regel ist der genaueste Weg, diese Informationen zu erhalten, der E-Mail-Administrator der Absenderorganisation zu kontaktieren. Wenn diese Ressource nicht vorhanden ist, können Sie eine der folgenden Optionen verwenden:

- **SenderBase:** Wenn Sie eine Domäne in das Suchfeld unter <http://www.senderbase.org> eingeben, erhalten Sie eine Liste der bekannten sendenden IP-Adressen für diese Domäne.
- **Mail-Protokolle** - Wenn Sie in der Vergangenheit erfolgreich E-Mails von der Domäne erhalten haben, können Sie in den Mail-Protokollen nach einer dieser erfolgreichen Lieferungen suchen.
- **Domain Name System (DNS)** - Sie können die Datensätze des Mail-Austausches (MX) für die Domäne durchsuchen. Die meisten kleineren Unternehmen verwenden dieselben Server für ein- und ausgehende Anrufe. Bei größeren oder stärker segmentierten Unternehmen werden die benötigten Informationen durch diese Option nicht preisgegeben.

Sobald Sie die IP-Adressen kennen, müssen Sie die E-Mail-Protokolle durchsuchen. Das grep-Dienstprogramm ist dafür ein gutes Tool. Wenn Sie Microsoft Windows ausführen, können Sie Find in Word Pad oder Notepad verwenden oder ein grep-Dienstprogramm aus dem Internet herunterladen. Unix und Mac OSX haben grep integriert und können von einer Shell aus aufgerufen werden. Die grep-Befehlszeile sieht wie folgt aus, wobei "10.2.3.4" die IP-Adresse ist, nach der gesucht werden soll:

```
host> grep '10.2.3.4' file.log
```

Wenn der Server des Absenders erfolgreich eine Verbindung zu Ihrem Server herstellt, wird eine Zeile angezeigt, die dem Beispiel in diesem Beispiel ähnelt, wenn Sie nach der IP-Adresse(n) suchen:

Wed Feb 2 23:43:11 2008 Info: New SMTP ICID 6 interface Management (10.0.0.1)
address 10.2.3.4 reverse dns host test.ironport.com verified no

Sie können dann nach allen Posten suchen, die die eingehende Verbindungs-ID (ICID) beinhalten. Die gesuchten Zeilen geben an, ob sie Informationen gesendet haben, ob sie an Informationen gesendet wurden und welche Nachrichten-IDs (MIDs) mit der Verbindung verknüpft sind. Eine Suche auf den MID(s) zeigt Ihnen, ob die Nachricht vom System akzeptiert wurde, die Prüfungsergebnisse und ob eine Zustellung versucht wurde.

Ein weiteres Tool zur Fehlerbehebung ist das **Injection Debug Logs**. Sie benötigen zuerst die IP-Adresse des/der sendenden Server(s). Sobald Sie diese haben, verwenden Sie die `logconfig` - Befehlen und wählen Sie diesen Protokolltyp aus. Nach der Konfiguration und Bestätigung des Protokolls kann der Benutzer eine Testnachricht senden lassen, und das Cisco Secure Email Gateway protokolliert die gesamte SMTP-Konversation (vorausgesetzt, der Server ist mit dem Cisco Secure Email Gateway verbunden). So können Sie den Punkt des Zusammenbruchs in der Kommunikation sehen.

Wenn immer noch keine Verbindungen vorhanden sind und somit keine Nachrichten empfangen werden, besteht der nächste Schritt darin, dass der Administrator der sendenden Server ihre Protokolle überprüft und/oder das Senden einer Nachricht vom Mail-Server mithilfe von Telnet manuell testen lässt. Dadurch wird der Server imitiert, der versucht, das Gerät an Ihr Cisco Secure Email Gateway zu senden, und Ihr Cisco Secure Email Gateway reagiert genauso, als ob die Anwendung, die die Server sendet, es gesendet hätte.

Wenn der Test erfolgreich verläuft, die Serveranwendung jedoch beim Senden von E-Mails ausfällt, weist dies auf Zustellungsprobleme auf dem Remote-Server hin. Der Remote-Serveradministrator muss die Protokolle überprüfen, um die Fehler zu diagnostizieren.

Eine häufige Ursache für den verzögerten oder fehlgeschlagenen Empfang von Nachrichten ist, dass die IP-Adresse des sendenden Servers nicht ordnungsgemäß für die DNS-Umkehr konfiguriert ist. Dies führt zu einer langen Verzögerung (30+ Sekunden), bis das Cisco Secure Email Gateway ein SMTP-Banner bereitstellt. Einige Serveranwendungen erreichen das konfigurierte Timeout und schließen die Sitzung, bevor sie E-Mails aufgrund des verzögerten Banners senden. In diesem Fall besteht die Lösung darin, die Zeitüberschreitung zu verlängern oder Reverse DNS zu implementieren. Empfohlen wird die Implementierung von Reverse DNS für alle Mail-Server, die an andere Internet-Mail-Server senden. Es wird als korrekte Internet-Etikette betrachtet und ermöglicht E-Mail-Servern, die Identität des Servers auf einer sehr einfachen Ebene zu bestätigen.