Wie kann ich die E-Mail-Protokolle auf der ESA durchsuchen und anzeigen?

Dokument-ID: 118552

Aktualisiert: 10. Oktober 2014

Unterstützt von Cisco TAC-Technikern.

Zugehörige Produkte

- Cisco Email Security Appliance

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie nach Protokolleinträgen suchen, die zeigen, wie die ESA (E-Mail Security Appliance) eine Nachricht verarbeitet hat.

Wie kann ich die E-Mail-Protokolle auf der ESA durchsuchen und anzeigen?

Sie können die Protokolle durchsuchen, um weitere Informationen über die *Von, An, Betreff* der E-Mails von dieser IP-Adresse zu sammeln, die Sie interessieren.

Der Name des Protokolls lautet *mail_logs*. Sie können dies unter **Systemverwaltung > Protokollabonnements > mail_logs** sehen.

Es gibt mehrere Möglichkeiten, auf diese Protokolle zuzugreifen.

1. Über den Webbrowser. Gehen Sie zu **Systemverwaltung > Protokollabonnement**.Für die

mail_logs klicken Sie auf den FTP-Link rechts neben mail_logs.Wenn Sie einen Fehler erhalten, gehen Sie zu **Netzwerk > IP-Schnittstelle**, wählen Sie die Schnittstelle aus, die Sie normalerweise auf die ESA zugreifen, und aktivieren Sie den FTP/Port 21-Dienst.

2. Über die Befehlszeile: Melden Sie sich mit einem SSH-Client wie Putty über Port 22/ssh an der CLI der ESA-Appliance an.Verwenden Sie in der Befehlszeile **grep**, um nach der IP zu suchen.Geben Sie die # ein, die den mail_logs Ihrer Appliance zugeordnet ist, und geben Sie dann das Suchmuster ein, d. h. 192.168.1.1 oder joe@example.com.Für die nächsten drei Fragen drücken Sie die Eingabetaste, und halten Sie die Standardeinstellungen gedrückt.Die Suche kann einige Zeit in Anspruch nehmen. Sobald die Ausgabe wiederhergestellt ist, können Sie entweder die ICID oder die MID durchsuchen.
   ```
   grep "ICID 123456" mail_logs
   ```
   Sobald die Ausgabe wiederhergestellt ist, können Sie nach der MID suchen.
   ```
   grep "MID 78901234" mail_logs
   ```
   Sie sollten den *Von, Bis, Betreff* aus der MID sehen können. Sie sollten die IP-Adresse und die HAT-Absendergruppe aus der ICID sehen.
3. Eine weitere Option besteht darin, die mail_logs auf ein lokales System (Desktop) zu laden und mit Ihrem eigenen Datei-/Texteditor nach den IP-Adressen zu suchen.

Ähnliche Diskussionen in der Cisco Support Community

Aktualisiert: 10. Oktober 2014
Dokument-ID: 118552