

# Häufig gestellte Fragen zur ESA: Was ist eine Mail Flow-Richtlinie?

## Inhalt

[Einführung](#)

[Was ist eine Mail Flow-Richtlinie?](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument werden die Richtlinien für den E-Mail-Fluss auf der E-Mail Security Appliance (ESA) und die Aktionen beschrieben, die einer Mail-Flow-Richtlinie zugeordnet sind.

## Was ist eine Mail Flow-Richtlinie?

Mit einer Mail Flow-Richtlinie können Sie den Fluss von E-Mail-Nachrichten von einem Sender zum Listener während der SMTP-Konversation steuern oder einschränken. Sie steuern SMTP-Konversationen, indem Sie die folgenden Parametertypen in der Mail-Fluss-Richtlinie definieren:

- Verbindungsparameter, z. B. die maximale Anzahl von Nachrichten pro Verbindung.
- Ratenlimitierungsparameter, z. B. maximale Anzahl von Empfängern pro Stunde.
- Ändern Sie benutzerdefinierte SMTP-Codes und -Antworten, die während der SMTP-Konversation kommuniziert werden.
- Aktivieren Sie die Spam-Erkennung.
- Aktivieren Sie den Virenschutz.
- Verschlüsselung, z. B. die Verwendung von TLS zur Verschlüsselung der SMTP-Verbindung.
- Authentifizierungsparameter, z. B. die Verwendung von DKIM zum Überprüfen eingehender E-Mails.

Mail-Flow-Richtlinien führen eine der folgenden Aktionen für Verbindungen von Remote-Hosts aus:

- **AKZEPTIEREN.** Die Verbindung wird akzeptiert, und die E-Mail-Aannahme wird dann durch die Listener-Einstellungen, einschließlich der RAT (Recipient Access Table) (für öffentliche Listener), weiter eingeschränkt.
- **ABLEHNEN.** Die Verbindung wird anfänglich akzeptiert, aber der Client, der eine Verbindung herstellt, erhält einen SMTP-Statuscode 4XX oder 5XX. Es wird keine E-Mail akzeptiert.

**Hinweis:** Sie können AsyncOS auch so konfigurieren, dass diese Ablehnung nicht zu Beginn der SMTP-Konversation, sondern auf der Ebene des Nachrichtenempfängers (RCPT TO) erfolgt. Wenn Nachrichten auf diese Weise zurückgewiesen werden, verzögert sich die

Nachrichtenabweisung, und die Nachricht wird abgesprengt. Dadurch kann AsyncOS detailliertere Informationen über die abgelehnten Nachrichten speichern. Diese Einstellung wird mit dem CLI-Befehl `listenerconfig > setup` konfiguriert.

- TCPREFUSE. Die Verbindung wird auf TCP-Ebene verweigert.
- RELAY. Verbindung wird akzeptiert. Die Annahme für einen Empfänger ist zulässig und nicht durch die RAT beschränkt.
- FORTFAHREN. Die Zuordnung in der Host Access Table (HAT) wird ignoriert, und die Verarbeitung der HAT wird fortgesetzt. Wenn die eingehende Verbindung mit einem späteren Eintrag übereinstimmt, der nicht CONTINUE ist, wird stattdessen dieser Eintrag verwendet. Die CONTINUE-Regel wird verwendet, um die Bearbeitung der HAT in der GUI zu vereinfachen.

Beachten Sie, dass Mail-Flow-Richtlinien am Anfang der E-Mail-Pipeline stehen. Diese Parameter werden angewendet, wenn Remote-Hosts versuchen, Verbindungen zur ESA herzustellen.

Mail Flow-Richtlinien unterscheiden sich von Incoming and Outgoing Mail Policies (Richtlinien für eingehende und ausgehende E-Mails), die Antispam-, Anti-Virus-, Virus-Outbreak- und Content-Filter-Parameter definieren, die auf E-Mails angewendet werden, die von bestimmten Domänen, Gruppen von E-Mail-Adressen oder bestimmten E-Mail-Adressen empfangen oder für diese bestimmt sind.

Die Standard-Mail Flow-Richtlinien können geändert und neue Mail Flow-Richtlinien definiert werden.

Für öffentliche Listener sind vier standardmäßige Mail-Flow-Richtlinien definiert:

- AKZEPTIERT
- GESPERRT
- DURCHGEFÜHRT
- VERTRAULICH

Private Listener verwenden die folgenden Mail-Flow-Richtlinien:

- AKZEPTIERT
- GESPERRT
- VERBUNDEN

## Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)