

Wie prüfe ich positiv identifizierte oder verdächtige Spam- und Marketing-E-Mails auf Fehlalarme?

Inhalt

[Einführung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Spam-Nachrichten, Marketing-E-Mails, die als positiv identifiziert wurden oder vermutet werden, auf Fehlalarme überprüft werden.

Wie prüfe ich positiv identifizierte oder verdächtige Spam- und Marketing-E-Mails auf Fehlalarme?

Die Cisco IronPort E-Mail Appliance (ESA) bietet mehrere Optionen, mit denen Sie Nachrichten speichern und falsch positive Anti-Spam-Verdicts untersuchen können.

In der GUI, **Mail-Policys > Mail-Policys für eingehende E-Mails** oder **Mail-Policys für "Ausgehend"** können Sie die Anti-Spam-Einstellungen für die Mail-Policy auswählen, um Spam-verdächtige Nachrichten oder Marketing-E-Mails an einen alternativen Host zu senden oder die IronPort Spam Quarantine (ISQ) zu senden.

Durch die Verwendung einer alternativen Hostadresse kann ein Administrator positiv identifizierte Spam-Nachrichten, Spam-verdächtige Nachrichten oder Marketing-E-Mails überprüfen und Fehlalarme melden.

Mit der ISQ können Administratoren und Endempfänger positiv identifizierte Spam, verdächtigen Spam oder Marketing-E-Mails überprüfen, bevor sie sie löschen oder freigeben.

Wenn falsche Positivmeldungen erkannt werden, melden Sie diese bitte an

ham@access.ironport.com.

Zugehörige Informationen

- [Häufig gestellte Fragen zur ESA: Wie meldet man Content Security Anti-Spam als Fehlalarm oder als Spam verpasste Nachrichten?](#)