Come fare per controllare messaggi di posta indesiderata sospetti o identificati in modo positivo, e-mail di marketing per individuare falsi positivi?

Sommario

Introduzione

In questo documento viene descritto come controllare la posta indesiderata sospetta o identificata in modo positivo, e-mail di marketing per rilevare eventuali falsi positivi.

Come fare per controllare messaggi di posta indesiderata sospetti o identificati in modo positivo, e-mail di marketing per individuare falsi positivi?

Cisco IronPort Email Appliance (ESA) offre diverse opzioni che consentono di archiviare i messaggi ed esaminare i verdetti anti-spam falsi positivi.

Nella GUI, **Mail Policies > Incoming Mail Policies** (Policy di posta in arrivo) o **Outgoing Mail Policies** (Policy di posta in uscita), scegliendo le impostazioni antispam per il criterio di posta, è possibile scegliere di inviare a un host alternativo la posta indesiderata identificata correttamente, la posta indesiderata sospetta o l'e-mail di marketing, oppure inviare l'ISQ (IronPort Spam Quarantine).

L'uso di un indirizzo host alternativo può consentire a un amministratore di esaminare messaggi indesiderati identificati correttamente, messaggi indesiderati sospetti o e-mail di marketing e segnalare eventuali falsi positivi.

L'ISQ consente sia agli amministratori che ai destinatari finali di esaminare le e-mail indesiderate identificate in modo positivo, sospette o di marketing prima di scegliere se eliminarle o rilasciarle.

Se vengono rilevati falsi positivi, segnalarli a ham@access.ironport.com.

Informazioni correlate

- Domande frequenti ESA: In che modo è possibile segnalare i falsi positivi o la mancata ricezione di posta indesiderata nella protezione dei contenuti?