Come risolvere i problemi relativi alla mancata ricezione di un messaggio da parte di Cisco Secure Email Gateway?

Sommario

Introduzione

In questo documento viene descritto il motivo per cui Cisco Secure Email Gateway non riceve un messaggio e vengono indicate le opzioni per risolvere il problema.

Come risolvere i problemi relativi alla mancata ricezione di un messaggio da parte di Cisco Secure Email Gateway?

Per risolvere i problemi relativi alla ricezione dei messaggi, è necessario conoscere gli indirizzi IP utilizzati dall'organizzazione che ha inviato la posta. In genere, il modo più accurato per ottenere queste informazioni consiste nel contattare l'amministratore della posta dell'organizzazione mittente. In assenza di questa risorsa, è possibile utilizzare una delle opzioni seguenti:

- **SenderBase** - Se si immette un dominio nella casella di ricerca all'indirizzo http://www.senderbase.org, si riceverà un elenco di indirizzi IP di invio noti per quel dominio.
- **Log di posta**: se la posta ricevuta dal dominio è stata correttamente ricevuta in passato, è possibile cercare nei log di posta uno di questi recapiti.
- **DNS (Domain Name System)** - È possibile cercare i record Mail Exchanger (MX) per il dominio. La maggior parte delle organizzazioni più piccole utilizza gli stessi server in entrata e in uscita. Per organizzazioni più grandi o più segmentate, questa opzione probabilmente non consente di visualizzare le informazioni necessarie.

Una volta che si conoscono gli indirizzi IP, sarà necessario ricercare nei log di posta. L'utilità grep è un ottimo strumento per questo scopo. Se si esegue Microsoft Windows, è possibile utilizzare Trova in Word Pad o Blocco note oppure scaricare un'utilità grep da Internet. Unix e Mac OSX dispongono di grep incorporato e sono accessibili da una shell. La riga di comando grep avrà questo aspetto, dove '10.2.3.4' è l'indirizzo IP da cercare:

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

Se il server del mittente si connette al server, quando si ricercano gli indirizzi IP verrà visualizzata una riga simile a quella riportata di seguito:

```
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
```

Èquindi possibile cercare tutte le righe che interessano l'ID connessione in ingresso (ICID). Nelle

righe trovate verrà indicato se sono state inviate le informazioni Da, se sono state inviate le informazioni A e gli ID messaggio (MID) collegati alla connessione. Una ricerca sui MID mostrerà se il messaggio è stato accettato dal sistema, i risultati dell'analisi e se è stato tentato il recapito.

Un altro strumento di risoluzione dei problemi disponibile è Injection Debug Logs (Registri di debug iniezione). È necessario innanzitutto l'indirizzo IP dei server di invio. Una volta ottenuto questo, utilizzare il **logconfig** e selezionare questo tipo di registro. Una volta configurato e confermato il log, è possibile fare in modo che l'utente invii un messaggio di prova e (presupponendo che il server si connetta a Cisco Secure Email Gateway) Cisco Secure Email Gateway registrerà l'intera conversazione SMTP. Ciò consente di vedere il punto di rottura nella comunicazione.

Se non vi sono ancora connessioni e quindi non viene ricevuto alcun messaggio, il passaggio successivo consiste nel richiedere all'amministratore dei server di invio di controllare i registri e/o utilizzare telnet per verificare manualmente l'invio di un messaggio dal server di posta. In questo modo il server tenterà di recapitare il messaggio a Cisco Secure Email Gateway e Cisco Secure Email Gateway reagirà come se fosse stato inviato dall'applicazione del server di invio.

Se il test viene superato, ma l'applicazione server non riesce quando tenta di inviare la posta, si verificano problemi di recapito sul server remoto. L'amministratore del server remoto dovrà esaminare i registri per diagnosticare gli errori.

Una causa comune del ritardo o della mancata ricezione dei messaggi è che l'indirizzo IP del server di invio non dispone di un DNS inverso configurato correttamente, il che causa un lungo ritardo (di oltre 30 secondi) perché Cisco Secure Email Gateway fornisca un banner SMTP. Alcune applicazioni server raggiungeranno il timeout configurato e chiuderanno la sessione prima dell'invio della posta a causa del posticipo del banner. In questo caso, la soluzione è estendere il timeout o implementare il DNS inverso. L'azione consigliata consiste nell'implementare il DNS inverso per tutti i server di posta che vengono recapitati ad altri server di posta Internet. Si ritiene che l'etichetta Internet sia adeguata e consente ai server di posta di confermare l'identità del server a un livello di base.