Quando un messaggio viene rilasciato dalla quarantena, dove viene registrato?

Sommario

Introduzione

In questo documento viene descritto come visualizzare i log di posta per determinare la disposizione di un messaggio rilasciato dalla quarantena su Cisco Email Security Appliance (ESA) o Cisco Security Management Appliance (SMA).

Quando un messaggio viene rilasciato dalla quarantena, dove viene registrato?

Sull'ESA, quando si rilascia un messaggio dall'ISQ (IronPort Spam Quarantine), dalla quarantena delle policy o da un'altra quarantena personalizzata, l'azione e l'evento associato vengono segnalati nel file di log di posta elettronica IronPort (mail_logs). La voce registrata nel log è collegata al MID originale.

Il modo migliore per risolvere il problema è ottenere *Da*, *A* o *Oggetto* del messaggio originale messo in quarantena. Quindi, cercarlo nel registro per vedere se è stato rilasciato dalla quarantena e quindi verificare se il server di posta finale l'ha accettato o rifiutato.

Esempio: ricerca nei log di posta del mittente "spam@test.com":

```
> grep -i "spam@test.com" mail_logs
Wed Aug 13 12:59:36 2014 Info: MID 1357 ICID 10152 From: <spam@test.com>
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: mailfrom identity spam@test.com None
Wed Aug 13 12:59:57 2014 Info: MID 1357 ready 185 bytes from <spam@test.com>
```

Prestare attenzione all'ID messaggio (MID) e all'ID connessione recapito (DCID).

Vediamo che questo particolare MID è stato inviato alla quarantena della posta indesiderata dai log di posta completi o dal monitoraggio dei messaggi:

```
Wed Aug 13 12:59:29 2014 Info: New SMTP ICID 10152 interface Management
(192.168.0.199) address 75.111.22.123 reverse dns host spam.test.com verified yes
Wed Aug 13 12:59:29 2014 Info: ICID 10152 RELAY SG RELAY_SG match 75.111.22.123
```

```
SBRS not enabled
Wed Aug 13 12:59:36 2014 Info: Start MID 1357 ICID 10152
Wed Aug 13 12:59:36 2014 Info: MID 1357 ICID 10152 From: <spam@test.com>
Wed Aug 13 12:59:40 2014 Info: MID 1357 ICID 10152 RID 0 To: <end_user@domain.com>
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: helo identity postmaster None
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: mailfrom identity spam@test.com None
Wed Aug 13 12:59:57 2014 Info: MID 1357 SPF: pra identity None headers None
Wed Aug 13 12:59:57 2014 Info: MID 1357 Message-ID '<9afe3f$1ad@my_esa.domain.com>'
Wed Aug 13 12:59:57 2014 Info: MID 1357 Subject 'This is spam?'
Wed Aug 13 12:59:57 2014 Info: MID 1357 ready 185 bytes from <spam@test.com>
Wed Aug 13 12:59:57 2014 Info: MID 1357 matched all recipients for per-recipient
policy DEFAULT in the outbound table
Wed Aug 13 12:59:58 2014 Info: MID 1357 interim verdict using engine: CASE
spam positive
Wed Aug 13 12:59:58 2014 Info: MID 1357 using engine: CASE spam positive
Wed Aug 13 12:59:58 2014 Info: ISQ: Tagging MID 1357 for quarantine
Wed Aug 13 12:59:58 2014 Info: MID 1357 interim AV verdict using Sophos CLEAN
Wed Aug 13 12:59:58 2014 Info: MID 1357 antivirus negative
Wed Aug 13 12:59:58 2014 Info: MID 1357 Outbreak Filters: verdict negative
Wed Aug 13 12:59:58 2014 Info: MID 1357 DLP no violation
Wed Aug 13 12:59:58 2014 Info: MID 1357 queued for delivery
Wed Aug 13 13:00:02 2014 Info: RPC Delivery start RCID 161 MID 1357 to local IronPort
Spam Quarantine
Wed Aug 13 13:00:08 2014 Info: ISQ: Quarantined MID 1357
Wed Aug 13 13:00:08 2014 Info: RPC Message done RCID 161 MID 1357
Wed Aug 13 13:00:08 2014 Info: Message finished MID 1357 done
Wed Aug 13 13:05:11 2014 Info: ICID 10152 close
```

Di seguito è riportato un esempio di ciò che è necessario cercare in un messaggio rilasciato dall'ISQ:

```
Wed Aug 13 13:02:14 2014 Info: Start MID 1359 ICID 0 (ISQ Released Message)
Wed Aug 13 13:02:14 2014 Info: ISQ: Reinjected MID 1357 as MID 1359
Wed Aug 13 13:02:14 2014 Info: MID 1359 ICID 0 From: <spam@test.com>
Wed Aug 13 13:02:14 2014 Info: MID 1359 ICID 0 RID 0 To: <end_user@domain.com>
Wed Aug 13 13:02:14 2014 Info: MID 1359 Subject '[SPAM] This is spam?'
Wed Aug 13 13:02:14 2014 Info: MID 1359 ready 1445 bytes from <spam@test.com>
Wed Aug 13 13:02:14 2014 Info: MID 1359 queued for delivery
Wed Aug 13 13:02:14 2014 Info: New SMTP DCID 165 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Aug 13 13:02:15 2014 Info: Delivery start DCID 165 MID 1359 to RID [0]
Wed Aug 13 13:02:15 2014 Info: Message done DCID 165 MID 1359 to RID [0]
Wed Aug 13 13:02:15 2014 Info: MID 1359 RID [0] Response '2.0.0 Ok: queued as
33B7380356'
Wed Aug 13 13:02:15 2014 Info: Message finished MID 1359 done
Wed Aug 13 13:02:20 2014 Info: DCID 165 close
```

Nell'esempio, il messaggio viene rilasciato e l'interfaccia (192.168.0.199) è il listener sull'ESA, che si connette a (192.168.0.200) come server di posta finale per il recapito.

Se si esaminano i log di quarantena della posta indesiderata (euq_logs), l'azione di rilascio mostra quanto segue:

```
Wed Aug 13 13:02:14 2014 Info: ISQ: Releasing MID [1357] for all
Wed Aug 13 13:02:14 2014 Info: ISQ: Delivering released MID 1357 (skipping
work queue)
Wed Aug 13 13:02:14 2014 Info: ISQ: Corpus status: 0
Wed Aug 13 13:02:15 2014 Info: ISQ: Released MID 1357 to end_user@domain.com
Wed Aug 13 13:02:15 2014 Info: ISQ: Deleting MID [1357] for all
Wed Aug 13 13:02:15 2014 Info: ISQ: Deleted MID 1357 for all
```

```
Wed Aug 13 13:02:15 2014 Info: ISQ: Cleared 8192 bytes (MIDs 1, for all
recipients) from database. Current bytes=0.
```

Analogamente, se il messaggio originale fosse stato messo in quarantena e poi rilasciato, si otterrebbe un risultato simile all'esempio seguente:

```
Wed Aug 13 13:09:27 2014 Info: MID 1361 released from quarantine "Policy" (manual)
t=29
Wed Aug 13 13:09:27 2014 Info: MID 1361 released from all quarantines
Wed Aug 13 13:09:27 2014 Info: MID 1361 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Aug 13 13:09:27 2014 Info: MID 1361 interim AV verdict using Sophos CLEAN
Wed Aug 13 13:09:27 2014 Info: MID 1361 antivirus negative
Wed Aug 13 13:09:27 2014 Info: MID 1361 queued for delivery
Wed Aug 13 13:09:27 2014 Info: New SMTP DCID 169 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Aug 13 13:09:27 2014 Info: Delivery start DCID 169 MID 1361 to RID [0]
Wed Aug 13 13:09:27 2014 Info: Message done DCID 169 MID 1361 to RID [0]
Wed Aug 13 13:09:27 2014 Info: MID 1361 RID [0] Response '2.0.0 Ok: queued
as C702980356'
Wed Aug 13 13:09:27 2014 Info: Message finished MID 1361 done
Wed Aug 13 13:09:32 2014 Info: DCID 169 close
```

Dalla quarantena della policy, il messaggio viene rilasciato dalla quarantena della policy, e l'interfaccia (192.168.0.199) è il listener sull'ESA, che si connette a (192.168.0.200) come server di posta finale per il recapito.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Che cos'è un ID messaggio (MID), un ID connessione di iniezione (ICID) o un ID connessione consegna (DCID)?
- Documentazione e supporto tecnico – Cisco Systems