Risoluzione dei problemi intermittenti e connessioni interrotte durante la ricezione e il recapito della posta

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi intermittenti e le connessioni interrotte durante la ricezione e il recapito della posta.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Private Internet eXchange (PIX) o Adaptive Security Appliance (ASA) versione 7.x e successive
- Cisco Email Security Appliance (ESA)

Premesse

I gateway e-mail Cisco ESA sono per loro natura firewall per la posta elettronica. Ciò elimina la necessità di un firewall a monte, come un Cisco PIX o ASA, per ispezionare il traffico di posta da e verso un'ESA. Si consiglia di disattivare le funzionalità di ispezione delle applicazioni ESMTP (Extended Simple Mail Transfer Protocol) sul firewall per qualsiasi indirizzo host dell'appliance di sicurezza. Per impostazione predefinita, l'ispezione del protocollo ESMTP è abilitata per tutte le connessioni che passano attraverso i firewall Cisco. Ciò significa che tutti i comandi emessi tra i gateway di posta tramite la porta TCP 25, nonché le singole intestazioni dei messaggi, vengono analizzati in modo da rispettare rigorosamente le specifiche RFC (Request for Comments) che includono gli standard RFC 821, 1123 e 1870. Sono stati definiti valori predefiniti per il numero

massimo di destinatari e le dimensioni dei messaggi che possono causare problemi di recapito da e verso l'ESA. Di seguito vengono riportati i valori predefiniti di configurazione (derivati dallo strumento di ricerca dei comandi Cisco).

Il comando **inspect esmtp** include le funzionalità precedentemente fornite dal comando **fixup smtp** e fornisce supporto aggiuntivo per alcuni comandi ESMTP. L'ispezione delle applicazioni ESMTP aggiunge il supporto per otto comandi ESMTP, tra cui AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML e **VRFY**. Oltre al supporto di sette comandi RFC 821 (DATA, HELO, MAIL, NOOP, QUIT, **RCPT**, **RSET**), l'appliance di sicurezza supporta un totale di 15 comandi SMTP. Altri comandi ESMTP, ad esempio ATRN, **STARTLS**, **ONEX**, **VERB**, **CHUNKING**, ed estensioni private non sono supportati. I comandi non supportati vengono convertiti in X, che vengono rifiutati dal server interno. Verrà visualizzato un messaggio del tipo **Comando 500 sconosciuto: XXX**. I comandi incompleti vengono eliminati.

Il comando **inspect esmtp** modifica i caratteri nel banner SMTP del server in asterischi, ad eccezione dei caratteri "2", "0", "0". I caratteri di ritorno a capo (CR) e avanzamento riga (LF) vengono ignorati. Se l'ispezione SMTP è attivata, una sessione utilizzata per SMTP interattivo attende un comando valido e il computer dello stato esmtp del firewall mantiene gli stati corretti per la sessione se queste regole non vengono rispettate:

- I comandi SMTP devono contenere almeno quattro caratteri.
- I comandi SMTP devono terminare con ritorno a capo e avanzamento riga.
- I comandi SMTP devono attendere una risposta prima di inviare la risposta successiva.

Un server SMTP risponde alle richieste dei client con codici di risposta numerici e stringhe facoltative leggibili. L'ispezione dell'applicazione SMTP controlla e riduce i comandi che l'utente può utilizzare, nonché i messaggi che il server restituisce. L'ispezione SMTP esegue tre attività principali:

- Limita le richieste SMTP a sette comandi SMTP di base e otto comandi estesi.
- Esegue il monitoraggio della sequenza di risposta dei comandi SMTP.
- Genera un audit trail. Il record di controllo 108002 viene generato quando viene sostituito un carattere non valido incorporato nell'indirizzo di posta. Per ulteriori informazioni, vedere la RFC 821.

Un'ispezione SMTP controlla il comando e la sequenza di risposta per individuare le firme anomale seguenti:

- Comandi troncati.
- Terminazione del comando non corretta (non terminata con <CR><LR>).
- Se la firma PIPE (PHY Interface for PCI Express) viene trovata come parametro di un comando **MAIL** from o **RCPT** to, la sessione viene chiusa. Non è configurabile dall'utente.
- Transizione imprevista dal server SMTP.
- Per i comandi sconosciuti, l'accessorio di protezione modifica tutti i caratteri del pacchetto in **X**. In questo caso, il server genererà un codice di errore per il client. A causa della modifica del pacchetto, il checksum TCP deve essere ricalcolato o modificato.
- Modifica di flussi TCP.

L'output di **show service-policy inspect ESMTP** fornisce i valori di ispezione predefiniti e le azioni corrispondenti.

```
Global policy:
Service-policy: global_policy
```

```
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Problema

Occasionalmente, i messaggi non verranno correttamente consegnati o ricevuti da Cisco ESA. Uno o più di questi messaggi sono visualizzati nei log di posta del dispositivo Cisco ESA:

- Messaggio interrotto MID XXX
- Ricezione interrotta ICID 21916 persa
- Chiusura ICID 21916
- Errore di connessione: DCID: Dominio XXX:example.com IP: 10.1.2.3 porta: 25 dettagli: [Errore 60]
  Interfaccia timeout operazione: 10.10.10.1 motivo: errore di rete

Soluzione

Alcune di queste impostazioni predefinite potrebbero influire su aspetti quali il recapito di messaggi crittografati TLS (Transport Layer Security), le campagne sulle liste di distribuzione e la risoluzione dei problemi. Una policy migliore potrebbe richiedere l'utilizzo del firewall per ispezionare tutto il traffico e-mail rimanente che non passa per la prima volta attraverso l'appliance di sicurezza, escludendo tutto il traffico che ha. In questo esempio viene illustrato come ottimizzare la configurazione predefinita (descritta in precedenza) per esentare l'ispezione delle applicazioni ESMTP per un singolo indirizzo host di sicurezza.

Èpossibile definire tutto il traffico da e verso l'indirizzo interno delle ESA Cisco per riferimento in una mappa di classe MPF (Modular Policy Framework):

```
access-list ironport_esa_internal extended permit ip any 192.168.1.1
access-list ironport_esa_internal extended permit ip 192.168.1.1 any
```

In questo modo viene creata una nuova mappa di classe per associare in modo specifico o

selezionare il traffico da gestire in modo diverso:

```
class-map ironport_esa
match address ironport_esa_internal
```

Questa sezione collega la nuova mappa delle classi Cisco e disabilita le funzionalità di ispezione del protocollo ESMTP:

```
policy-map global_policy
class ironport_esa
no inspect esmtp
```

Notare anche l'istruzione di traduzione dell'indirizzo che può aiutare a controllare il numero di connessioni in entrata e parzialmente aperte (embrionali) all'indirizzo. Ciò è utile per combattere gli attacchi DoS (Denial of Service), ma può interferire con le velocità di consegna.

Formattare per tracciare i parametri dei comandi **NAT** e **STATIC** ... [tcp (max_conns)] [max_embrionic].
In questo esempio vengono specificati i limiti di 50 connessioni TCP totali e di 100 tentativi di connessione half-open o embrionali:

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```