Risoluzione dei problemi comuni di HAT/RAT sull'ESA

Sommario

Introduzione

In questo documento viene fornita una panoramica di alto livello, le linee guida per la configurazione e le tecniche di risoluzione dei problemi per diagnosticare i problemi comuni relativi a Host Access Table (HAT) e Recipient Access Table (RAT) su Email Security Appliance (ESA).

Panoramica

CAPPELLO

Per ogni listener configurato, è necessario definire un set di regole che controllino le connessioni in ingresso dagli host remoti. Ad esempio, è possibile definire gli host remoti e stabilire se possono o meno connettersi al listener. AsyncOS consente di definire gli host autorizzati a connettersi al

listener utilizzando HAT.

HAT gestisce un set di regole che controllano le connessioni in ingresso dagli host remoti per un listener. Ogni listener configurato ha il proprio HAT indipendente. È possibile configurare gli HAT sia per i listener pubblici che per quelli privati.

Per impostazione predefinita, la funzione HAT prevede azioni diverse a seconda del tipo di listener:

- Listener pubblico: HAT è configurato per accettare messaggi di posta elettronica da tutti gli host.
- Listener privato: HAT è configurato per inoltrare la posta elettronica dagli host specificati e rifiutare tutti gli altri host.

Una regola HAT è costituita da un gruppo di mittenti, un punteggio SBRS (SenderBase Reputation Score), origini feed minacce esterne applicate e criteri flusso di posta.

Gruppo mittente

Un gruppo di mittenti è un elenco di mittenti identificati da uno o più di questi:

- Indirizzo IP (IPv4 o IPv6)
- Intervallo IP
- Nome host o dominio specifico
- Classificazione 'organizzazione' servizio reputazione IP
- Intervallo (o mancanza di punteggio) del punteggio IP Reputation Score (IPRS)
- Risposta query elenco DNS

Punteggio reputazione SenderBase

L'appliance può eseguire una query sul servizio di reputazione IP per determinare un punteggio di reputazione IP. Il punteggio di reputazione IP è un valore numerico assegnato a un indirizzo IP, a un dominio o a un'organizzazione in base alle informazioni fornite dal servizio di reputazione IP.

Origini ETF (External Threat Feed) applicate

Il quadro ETF consente all'ESA di utilizzare le informazioni sulle minacce esterne in formato STIX comunicate tramite il protocollo TAXII.

La capacità di utilizzare le informazioni sulle minacce esterne consente all'organizzazione di:

- Rispondere in modo proattivo a minacce informatiche quali malware, ransomware, attacchi di phishing e attacchi mirati.
- Iscriviti a fonti di intelligence sulle minacce locali e di terze parti.
- Maggiore efficacia.

Per utilizzare ETF sull'ESA è necessaria una chiave di funzione valida. Per informazioni su come ottenere una chiave funzione, contattare il rappresentante commerciale Cisco e/o Cisco Global Licensing Operations.

Criteri flusso di posta

I criteri di flusso della posta consentono di controllare o limitare il flusso dei messaggi di posta elettronica da un mittente al listener durante la conversazione SMTP. È possibile controllare le conversazioni SMTP definendo questi tipi di parametri nei criteri di flusso della posta:

- Parametri di connessione (ad esempio, numero massimo di messaggi per connessione)
- Parametri di limitazione della velocità (ad esempio, numero massimo di destinatari all'ora)
- I codici e le risposte SMTP personalizzati vengono comunicati durante la conversazione SMTP
- Abilita/disabilita rilevamento posta indesiderata
- Attivare/disattivare la protezione antivirus
- Crittografia (ad esempio, TLS)
- Autenticazione e verifica (ad esempio, DMARC, DKIM e SPF)

RATTO

AsyncOS utilizza l'RAT per ogni listener pubblico per gestire l'accettazione o il rifiuto degli indirizzi dei destinatari. Gli indirizzi dei destinatari includono:

- Domini
- Indirizzi di posta elettronica
- Gruppi di indirizzi di posta elettronica

Per impostazione predefinita, l'RAT rifiuta tutti i destinatari per impedire la creazione di un inoltro aperto.

Scenari di implementazione comuni

Blocco manuale di un mittente

Per bloccare un mittente specifico in base all'indirizzo IP del mittente, aggiungere una voce manuale per l'indirizzo IP nel gruppo di mittenti dell'elenco di blocco e verificare che l'azione sia impostata su 'Rifiuta' o 'Rifiuta TCP'. Per istruzioni sulla configurazione, consultare: Blocco manuale di un indirizzo IP mittente sull'ESA.

Aggiunta di gruppi/intervalli di indirizzi IP al servizio HAT

Gli indirizzi IP adiacenti possono essere raggruppati come subnet, ad esempio 192.0.2.0/24, intervalli di indirizzi IP, ad esempio 192.0.2.10-20, oppure indirizzi IP parziali, ad esempio 192.0.2., e aggiunti alla tabella. Per aggiungere più indirizzi IP non adiacenti, attenersi alla seguente procedura:

Dall'interfaccia grafica:

1. Passare a Mail Policies > HAT Overview (Policy di posta > Panoramica HAT) (se necessario, scegliere il livello cluster appropriato).
2. Scegliere il gruppo di mittenti da modificare e scegliere Aggiungi mittente.
3. Nel campo Sender (Mittente), immettere gli intervalli IP applicabili (ad esempio, 192.0.2.0/24), un commento facoltativo, quindi scegliere Submit (Invia).
4. Fare clic su Commit modifiche per salvare.

Dalla CLI:

1. Eseguire la sequenza di comandi:

   <#root>

   ```
   listenerconfig >> EDIT
   ```

2. Immettere il nome o il numero del listener da modificare.
3. Eseguire la sequenza di comandi e quindi immettere il numero o il nome del gruppo di mittenti da modificare:

   ```
   HOSTACCESS >> EDIT >> 1
   ```

4. Scegliere nuovo e immettere un elenco di mittenti separati da virgole da aggiungere.

5. Al termine, eseguire il comando commit per salvare le modifiche.

Risoluzione dei problemi

Mittente Corrispondente Al Gruppo Mittenti Non Corretto

Verificare i log di posta sull'ESA o la verifica dei messaggi su Security Management Appliance (SMA) e verificare la presenza di queste voci nell'ICID (Incoming Connection ID):

```
ICID 476946 ACCEPT SG WhiteList match nx.example SBRS None country United States
```

Motivo: La verifica DNS dell'host connesso è abilitata nel gruppo di mittenti e la connessione del record PTR dell'host non esiste nel DNS è selezionata.

```
ICID 476946 ACCEPT SG WhiteList match not.double.verified.example SBRS None country United States
```

Motivo: La verifica DNS dell'host è abilitata nel gruppo di mittenti e la connessione della ricerca DNS inversa (PTR) dell'host non corrisponde alla ricerca DNS diretta (A) scelta.

```
ICID 476946 ACCEPT SG WhiteList match serv.fail.example SBRS None country United States
```

Motivo: La verifica DNS dell'host è abilitata nel gruppo di mittenti e la connessione della ricerca dei record PTR dell'host non è riuscita a causa di un errore DNS temporaneo è selezionata.

Configurazione dell'host del gruppo di mittenti errata

Un gruppo di mittenti è un elenco di mittenti identificato da:

- Indirizzo IP (IPv4 o IPv6)
- Intervallo IP
- Nome host o dominio specifico
- Classificazione 'organizzazione' servizio reputazione IP
- Intervallo (o mancanza di punteggio) del punteggio IP Reputation Score (IPRS)
- Risposta query elenco DNS

Esempio di indirizzi configurati in modo errato nel gruppo mittente: il gruppo mittente ESA corrisponde a nomi host parziali.

I rifiuti HAT/RAT vengono conteggiati in base a 'Fermati dal filtro reputazione'?

Sì, i messaggi rifiutati da un gruppo di mittenti con l'azione di rifiuto nei criteri di flusso della posta vengono conteggiati nel contatore di report 'Interrotto da filtro reputazione'.

Nota: Questo contatore può includere rifiuti di criteri HAT e rifiuti basati su SBRS. Verificare il motivo del rifiuto nei log di posta per distinguere l'origine.

Verifica dei rifiuti in base alla tabella RAT

Questo è un esempio di output di log dai log di posta su un ESA:

```
Thu Sep 18 09:10:14 2014 Info: MID 48445 ICID 15970 To: <user@example.com> "Rejected by RAT"
```

Motivo: Il dominio specifico non è consentito in RAT nella configurazione ESA.

Come registrare ulteriori informazioni su mittente/destinatario per le connessioni rifiutate?

Per impostazione predefinita, una connessione rifiutata registra nei log di posta solo l'indirizzo IP dell'MTA del mittente e non registra il mittente o il destinatario della busta. Se per la risoluzione dei problemi è necessaria una registrazione aggiuntiva, è possibile abilitare il rifiuto HAT ritardato su AsyncOS.

Attenzione: Cisco consiglia di non abilitare questa funzione in modo permanente perché richiede ulteriori risorse.

Ulteriori dettagli sono disponibili qui: HAT Delayed Rejection FAQ.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).