Fehlerbehebung bei häufigen HAT/RAT-Fehlern auf der ESA

Inhalt

- Einleitung
- Überblick
  - HUT
  - Absendergruppe
  - SenderBase-Reputationsbewertung
  - Angewandte externe Bedrohungs-Feed-Quellen (ETF)
  - Mail Flow-Richtlinie
  - RATE
- Gängige Implementierungsszenarien
  - Manuelles Sperren von Absendern
  - Hinzufügen von Gruppen/Bereichen von IP-Adressen zur HAT
- Fehlerbehebung
  - Absenderzuordnung: Falsche Absendergruppe
  - Falsche Absendergruppen-Hostkonfiguration
  - Zählen HAT/RAT-Ablehnungen auf 'Stopped by Reputation Filtering'?
  - Zurückweisungen nach RAT-Tabelle überprüfen
  - Wie werden zusätzliche Absender-/Empfängerinformationen für abgelehnte Verbindungen protokolliert?
- Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt eine grobe Übersicht, Konfigurationsanleitungen und Fehlerbehebungsverfahren zur Diagnose häufiger Probleme in der Host Access Table (HAT) und Recipient Access Table (RAT) der E-Mail Security Appliance (ESA).

Überblick

HUT

Für jeden konfigurierten Listener müssen Sie einen Satz von Regeln definieren, die eingehende Verbindungen von Remote-Hosts steuern. Sie können beispielsweise Remote-Hosts definieren und festlegen, ob diese eine Verbindung mit dem Listener herstellen können. Mit AsyncOS

können Sie definieren, welche Hosts mithilfe der HAT eine Verbindung zum Listener herstellen dürfen.

Die HAT verwaltet einen Satz von Regeln, die eingehende Verbindungen von Remote-Hosts für einen Listener steuern. Jeder konfigurierte Listener verfügt über eine eigene unabhängige HAT. Sie können HATs für öffentliche und private Listener konfigurieren.

Standardmäßig wird die HAT so definiert, dass je nach Listener-Typ unterschiedliche Aktionen ausgeführt werden:

- Öffentlicher Listener: Die HAT ist so eingerichtet, dass sie E-Mails von allen Hosts akzeptiert.
- Privater Listener: Die HAT ist so konfiguriert, dass sie E-Mails von den von Ihnen angegebenen Hosts weiterleitet und alle anderen Hosts ablehnt.

Eine HAT-Regel besteht aus einer Absendergruppe, einer SenderBase-Reputationsbewertung (SBRS), angewendeten externen Bedrohungs-Feed-Quellen und einer Mail Flow Policy.

Absendergruppe

Eine Absendergruppe ist eine Liste von Absendern, die durch einen oder mehrere der folgenden Punkte identifiziert werden:

- IP-Adresse (IPv4 oder IPv6)
- IP-Bereich
- Spezifischer Host- oder Domänenname
- IP-Reputationsdienst-Organisationsklassifizierung
- IP Reputation Score (IPRS)-Bereich (oder keine Bewertung)
- DNS-Listenabfrageantwort

SenderBase-Reputationsbewertung

Die Appliance kann den IP-Reputationsdienst abfragen, um eine IP-Reputationsbewertung zu ermitteln. Bei der IP-Reputationsbewertung handelt es sich um einen numerischen Wert, der einer IP-Adresse, Domäne oder Organisation basierend auf Informationen vom IP-Reputationsdienst zugewiesen wird.

Angewandte externe Bedrohungs-Feed-Quellen (ETF)

Das ETF-Framework ermöglicht der ESA die Nutzung externer Bedrohungsinformationen im STIX-Format, die über das TAXII-Protokoll übermittelt werden.

Die Nutzung externer Bedrohungsinformationen bietet folgende Vorteile:

- Proaktive Reaktion auf Cyber-Bedrohungen wie Malware, Ransomware, Phishing-Angriffe und zielgerichtete Angriffe
- Abonnieren Sie lokale Threat-Intelligence und Threat-Intelligence von Drittanbietern.
- Steigerung der Effizienz.

Sie benötigen einen gültigen Feature-Schlüssel, um ETF auf Ihrer ESA verwenden zu können. Informationen zum Anfordern eines Feature-Schlüssels erhalten Sie von Ihrem Ansprechpartner bei Cisco und/oder bei Cisco Global Licensing Operations.

Mail Flow-Richtlinie

Mail Flow-Richtlinien ermöglichen Ihnen, den Fluss von E-Mail-Nachrichten von einem Absender zum Listener während der SMTP-Konversation zu steuern oder einzuschränken. Sie steuern SMTP-Konversationen, indem Sie diese Parametertypen in der Mail Flow Policy definieren:

- Verbindungsparameter (z. B. maximale Anzahl Nachrichten pro Verbindung)
- Parameter für die Ratenbegrenzung (z. B. die maximale Anzahl von Empfängern pro Stunde)
- Benutzerdefinierte SMTP-Codes und -Antworten werden während der SMTP-Konversation kommuniziert.
- Anti-Spam-Erkennung aktivieren/deaktivieren
- Antivirus-Schutz aktivieren/deaktivieren
- Verschlüsselung (z. B. TLS)
- Authentifizierung und Verifizierung (z. B. DMARC, DKIM und SPF)

RATE

AsyncOS verwendet die RAT für jeden öffentlichen Listener, um die Annahme oder Ablehnung von Empfängeradressen zu verwalten. Zu den Empfängeradressen gehören:

- Domänen
- E-Mail-Adressen
- Gruppen von E-Mail-Adressen

Standardmäßig lehnt die RAT alle Empfänger ab, um die Erstellung eines offenen Relays zu verhindern.

Gängige Implementierungsszenarien

Manuelles Sperren von Absendern

Um einen bestimmten Absender nach Absender-IP-Adresse zu blockieren, fügen Sie einen manuellen Eintrag für die IP-Adresse in der Absendergruppe in der Sperrliste hinzu, und stellen Sie sicher, dass die Aktion auf "Reject" (Ablehnen) oder "TCP Refuse" (TCP ablehnen) gesetzt ist. Konfigurationsanweisungen finden Sie unter Manuelles Sperren einer Absender-IP auf der ESA.

Hinzufügen von Gruppen/Bereichen von IP-Adressen zur HAT

Benachbarte IP-Adressen können als Subnetze wie 192.0.2.0/24, IP-Adressbereiche wie 192.0.2.10-20 oder partielle IP-Adressen wie 192.0.2 gruppiert und der Tabelle hinzugefügt werden. Um mehrere nicht benachbarte IP-Adressen hinzuzufügen, gehen Sie wie folgt vor:

Über die GUI:

1. Navigieren Sie zu Mail-Policys > HAT-Übersicht (wählen Sie ggf. die entsprechende Cluster-Ebene aus).
2. Wählen Sie die zu ändernde Absendergruppe aus, und wählen Sie Absender hinzufügen aus.
3. Geben Sie im Feld Absender die entsprechenden IP-Bereiche (z. B. 192.0.2.0/24) und einen optionalen Kommentar ein, und wählen Sie Senden.
4. Klicken Sie zum Speichern auf Änderungen bestätigen.

Über die CLI:

1. Führen Sie die folgende Befehlssequenz aus:

   <#root>

   listenerconfig >> EDIT

2. Geben Sie den Namen oder die Nummer des zu bearbeitenden Listeners ein.
3. Führen Sie die Befehlssequenz aus, und geben Sie dann die Nummer oder den Namen der Absendergruppe ein, die bzw. den Sie bearbeiten möchten:

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

4. Wählen Sie new aus, und geben Sie eine kommagetrennte Liste der hinzuzufügenden Absender ein.
5. Wenn Sie fertig sind, führen Sie commit aus, um die Änderungen zu speichern.

Fehlerbehebung

Absenderzuordnung: Falsche Absendergruppe

Überprüfen Sie die E-Mail-Protokolle auf der ESA oder die Nachrichtenverfolgung auf der Security Management Appliance (SMA), und überprüfen Sie die Eingangsverbindungs-ID (ICID) auf folgende Einträge:

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

Grund: Die DNS-Verifizierung des verbindenden Hosts ist für die Absendergruppe aktiviert, und der PTR-Eintrag des verbindenden Hosts ist in DNS nicht vorhanden ist wurde ausgewählt.

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

Grund: Die DNS-Verifizierung des verbindenden Hosts ist für die Absendergruppe aktiviert, und die umgekehrte DNS-Suche (PTR) des verbindenden Hosts stimmt nicht mit der vorwärts gerichteten DNS-Suche (A) überein.

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

Grund: Die DNS-Verifizierung des verbindenden Hosts ist für die Absendergruppe aktiviert, und die PTR-Suche des verbindenden Hosts schlägt aufgrund eines temporären DNS-Fehlers fehl.

Falsche Absendergruppen-Hostkonfiguration

Eine Absendergruppe ist eine Liste von Absendern, die identifiziert wird durch:

- IP-Adresse (IPv4 oder IPv6)
- IP-Bereich
- Spezifischer Host- oder Domänenname
- IP-Reputationsdienst-Organisationsklassifizierung
- IP Reputation Score (IPRS)-Bereich (oder keine Bewertung)
- DNS-Listenabfrageantwort

Beispiel für falsch konfigurierte Adressen unter Absendergruppe: ESA-Absendergruppe, die partielle Hostnamen vergleicht.

Zählen HAT/RAT-Ablehnungen auf 'Stopped by Reputation Filtering'?

Ja, Nachrichten, die von einer Absendergruppe mit der Ablehnungsaktion in der Mail Flow Policy zurückgewiesen wurden, werden im Berichtszähler "Stopped by Reputation Filtering" gezählt.

Anmerkung: Dieser Leistungsindikator kann Ablehnungen von HAT-Richtlinien und SBRS-basierte Ablehnungen enthalten. Überprüfen Sie den Ablehnungsgrund in den Mail-Protokollen, um die Quelle zu identifizieren.

Zurückweisungen nach RAT-Tabelle überprüfen

Dies ist ein Beispiel für die Protokollausgabe von E-Mail-Protokollen auf einer ESA:

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

Grund: Die spezifische Domäne ist unter RAT in der ESA-Konfiguration nicht zulässig.

Wie werden zusätzliche Absender-/Empfängerinformationen für abgelehnte Verbindungen protokolliert?

Standardmäßig protokolliert eine abgelehnte Verbindung nur die MTA-IP-Adresse des Absenders in den E-Mail-Protokollen und nicht den Absender oder Empfänger des Umschlags. Wenn zur Fehlerbehebung zusätzliche Protokollierung erforderlich ist, kann bei AsyncOS die verzögerte HAT-Ablehnung aktiviert werden.

⚠

> Vorsicht: Cisco empfiehlt, diese Funktion nicht dauerhaft zu aktivieren, da hierfür zusätzliche Ressourcen erforderlich sind.

Weitere Informationen finden Sie hier: HAT Verzögerte Ablehnung FAQ.

Zugehörige Informationen

- Cisco Email Security Appliance – Endbenutzerhandbücher
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.