Problemen oplossen met veelvoorkomende HAT/RAT-fouten op ESA

Inhoud

Inleiding

Dit document beschrijft een overzicht op hoog niveau, configuratierichtlijnen en technieken voor probleemoplossing om veelvoorkomende problemen voor de Host Access Table (HAT) en de Recipient Access Table (RAT) op de Email Security Appliance (ESA) te diagnosticeren.

Overzicht

HOED

Voor elke geconfigureerde listener moet u een reeks regels definiëren die inkomende verbindingen vanaf externe hosts regelen. U kunt bijvoorbeeld externe hosts definiëren en bepalen of deze verbinding kunnen maken met de listener. Met AsyncOS kunt u bepalen welke

hosts met de HAT verbinding mogen maken met de luisteraar.

De HAT onderhoudt een set regels die binnenkomende verbindingen van externe hosts voor een luisteraar regelen. Elke geconfigureerde luisteraar heeft zijn eigen onafhankelijke HAT. U kunt HAT's configureren voor zowel publieke als private luisteraars.

Standaard is de HAT gedefinieerd om verschillende acties uit te voeren, afhankelijk van het type listener:

- Publieke luisteraar: De HAT is ingesteld om e-mails van alle hosts te accepteren.
- Privé-listener: De HAT is geconfigureerd om e-mail door te sturen van de host(s) die u opgeeft en alle andere hosts te weigeren.

Een HAT-regel bestaat uit een Sender Group, SenderBase Reputation Score (SBRS), externe bronnen voor dreigingsinvoer die zijn toegepast en het e-mailstroombeleid.

zendergroep

Een afzendergroep is een lijst van afzenders die door een of meer van deze:

- IP-adres (IPv4 of IPv6)
- IP-bereik
- Specifieke host- of domeinnaam
- IP Reputation Service 'organisatie' classificatie
- IP Reputation Score (IPRS) bereik (of gebrek aan score)
- DNS-lijstqueryrespons

SenderBase-reputatiescore

Het toestel kan de IP-reputatieservice bevragen om een IP-reputatiescore te bepalen. De IP-reputatiescore is een numerieke waarde die wordt toegewezen aan een IP-adres, domein of organisatie op basis van informatie van de IP-reputatieservice.

Externe dreigingsfeed (ETF) bronnen toegepast

Het ETF-kader stelt de ESA in staat om informatie over externe bedreigingen in STIX-formaat te gebruiken, die via het TAXII-protocol wordt meegedeeld.

De mogelijkheid om informatie over externe bedreigingen te consumeren, helpt een organisatie

om:

- Proactief reageren op cyberdreigingen zoals malware, ransomware, phishing-aanvallen en gerichte aanvallen.
- Abonneer u op lokale en externe bronnen van bedreigingsinformatie.
- Verbetert de effectiviteit.

U hebt een geldige functietoets nodig om ETF op uw ESA te gebruiken. Neem contact op met uw Cisco-vertegenwoordiger en/of Cisco Global Licensing Operations voor informatie over het verkrijgen van een functietoets.

e-mailstroombeleid

Met e-mailstroombeleid kunt u de stroom e-mailberichten van een afzender naar de luisteraar tijdens het SMTP-gesprek regelen of beperken. U beheert SMTP-gesprekken door dit soort parameters te definiëren in het e-mailstroombeleid:

- Verbindingsparameters (bijvoorbeeld maximaal aantal berichten per verbinding)
- Tariefbeperkende parameters (bijvoorbeeld maximaal aantal ontvangers per uur)
- Aangepaste SMTP-codes en antwoorden worden gecommuniceerd tijdens het SMTP-gesprek
- Anti-spam detectie in-/uitschakelen
- Antivirusbeveiliging in-/uitschakelen
- Encryptie (bijvoorbeeld TLS)
- Authenticatie en verificatie (bijvoorbeeld DMARC, DKIM en SPF)

RAT

AsyncOS gebruikt de RAT voor elke openbare luisteraar om de acceptatie of afwijzing van ontvangers te beheren. Adressen van geadresseerden omvatten deze:

- Domeinen
- E-mailadressen
- Groepen e-mailadressen

Standaard wijst de RAT alle ontvangers af om het aanmaken van een open relais te voorkomen.

Gemeenschappelijke implementatiescenario's

Een afzender handmatig blokkeren

Om een specifieke afzender te blokkeren door het IP-adres van de afzender, voeg een handmatige vermelding voor het IP-adres toe onder de afzendergroep van de blokkeerlijst en zorg ervoor dat de actie is ingesteld op 'Afwijzen' of 'TCP weigeren'. Voor configuratie-instructies raadpleegt u: Een afzender-IP handmatig blokkeren op ESA.

Groepen/bereiken van IP-adressen toevoegen aan de HAT

Aangrenzende IP-adressen kunnen worden gegroepeerd als subnetten zoals 192.0.2.0/24, IP-adresbereiken zoals 192.0.2.10-20 of gedeeltelijke IP-adressen zoals 192.0.2. en toegevoegd aan de tabel. Als u meerdere niet-aangrenzende IP-adressen wilt toevoegen, voert u de volgende stappen uit:

Via de GUI:

1. Navigeer naar Mail Policies > HAT Overview (kies indien nodig het juiste clusterniveau).
2. Kies de afzendergroep die u wilt wijzigen en kies Afzender toevoegen.
3. Voer in het veld Afzender de toepasselijke IP-bereiken in (bijvoorbeeld 192.0.2.0/24), een optionele opmerking en kies Indienen.
4. Klik op Wijzigingen vastleggen om op te slaan.

Vanuit de CLI:

1. Voer de opdrachtvolgorde uit:

   <#root>

   listenerconfig >> EDIT

2. Voer de naam of het nummer in van de te bewerken listener.
3. Voer de opdrachtvolgorde uit en voer vervolgens het afzendergroepnummer of de naam in die u wilt bewerken:

   HOSTACCESS >> EDIT >> 1

4. Kies nieuw en voer een door komma's gescheiden lijst met afzenders in om toe te voegen.
5. Als u klaar bent, voert u commit uit om de wijzigingen op te slaan.

Probleemoplossing

Afzender komt overeen met verkeerde afzendergroep

Controleer de e-maillogboeken op de ESA of de berichttracering op de Security Management Appliance (SMA) en controleer of deze gegevens in de Incoming Connection ID (ICID) staan:

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

Reden: Verbinding maken met host-DNS-verificatie is ingeschakeld in de groep van de afzender en verbinding maken met host-PTR-record bestaat niet in DNS is geselecteerd.

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

Reden: Het verbinden van host-DNS-verificatie is ingeschakeld in de afzendergroep en het verbinden van host reverse DNS lookup (PTR) komt niet overeen met de forward DNS lookup (A) wordt gekozen.

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

Reden: Verbinding maken met host-DNS-verificatie is ingeschakeld in de afzendergroep en het zoeken naar host-PTR-records mislukt als gevolg van een tijdelijke DNS-fout is geselecteerd.

Onjuiste configuratie van afzendergroep-host

Een afzendergroep is een lijst van afzenders die worden geïdentificeerd door:

- IP-adres (IPv4 of IPv6)
- IP-bereik
- Specifieke host- of domeinnaam
- IP Reputation Service 'organisatie' classificatie
- IP Reputation Score (IPRS) bereik (of gebrek aan score)
- DNS-lijst queryrespons

Voorbeeld van verkeerd geconfigureerde adressen onder Sender Group: ESA Sender Group Matching Partial Hostnames.

Tellen HAT/RAT-afwijzingen mee bij 'Stopped by Reputation Filtering'?

Ja, berichten die zijn afgewezen door een afzendergroep met de afwijzingsactie in het e-mailstroombeleid, worden geteld in de rapportteller 'Gestopt door reputatiefiltering'.

Opmerking: deze teller kan afwijzingen van HAT-beleid en op SBRS gebaseerde afwijzingen bevatten. Controleer de reden voor afwijzing in de maillogboeken om de bron te onderscheiden.

Afwijzingen controleren op RAT-tabel

Dit is een voorbeeld van loguitvoer uit de maillogboeken op een ESA:

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

Reden: Het specifieke domein is niet toegestaan onder de RAT in de ESA-configuratie.

Hoe logt u aanvullende afzender-/ontvangstgegevens voor geweigerde verbindingen?

Standaard logt een geweigerde verbinding alleen het MTA-IP-adres van de afzender in de maillogboeken en logt de afzender van de enveloppe of de ontvanger van de enveloppe niet. Als extra logboekregistratie vereist is voor het oplossen van problemen, kan vertraagde HAT-weigering worden ingeschakeld op AsyncOS.

Let op: Cisco raadt u aan deze functie niet permanent in te schakelen omdat hiervoor extra bronnen nodig zijn.

Meer details zijn hier te vinden: HAT Delayed Rejection FAQ.

Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.