Op snelheid gebaseerde aanvalspreventie configureren met Snort 3-snelheidsfilter op beveiligde FTD

uitgeven

De focus ligt op het structureren van regels om meerdere subnetten te bestrijken, het begrijpen van best practices voor implementatie en het bepalen van passende drempelwaarden (aantal per seconde) voor alarmering of blokkering, met name in de context van SYN-overstromingsaanvalpreventie.

milieu

- Cisco Secure Firewall Firepower met FTD 7.4.2.4
- Firepower 2110-hardwareplatform
- Beheerd door Firepower Management Center (FMC) 7.6.2.1
- Snort 3 Inbraakpreventiesysteem met rate_filter-inspector ingeschakeld
- Meerdere interne subnetten die bescherming behoeven tegen SYN-overstromingen
- Geen actieve fouten aanwezig; configuratierichtlijnen voor proactieve verdediging

resolutie

In deze stappen wordt beschreven hoe u op snelheid gebaseerde aanvalspreventie kunt configureren en implementeren met behulp van de Snort 3 rate_filter-inspector op Cisco Secure Firewall FTD, inclusief een uitleg van de regelstructuur voor meerdere subnetten en aanbevelingen voor beste praktijken. Deze acties zijn bedoeld om basislijnen voor normaal verkeer vast te stellen en om SYN-overstromingsaanvallen effectief te detecteren of te blokkeren.

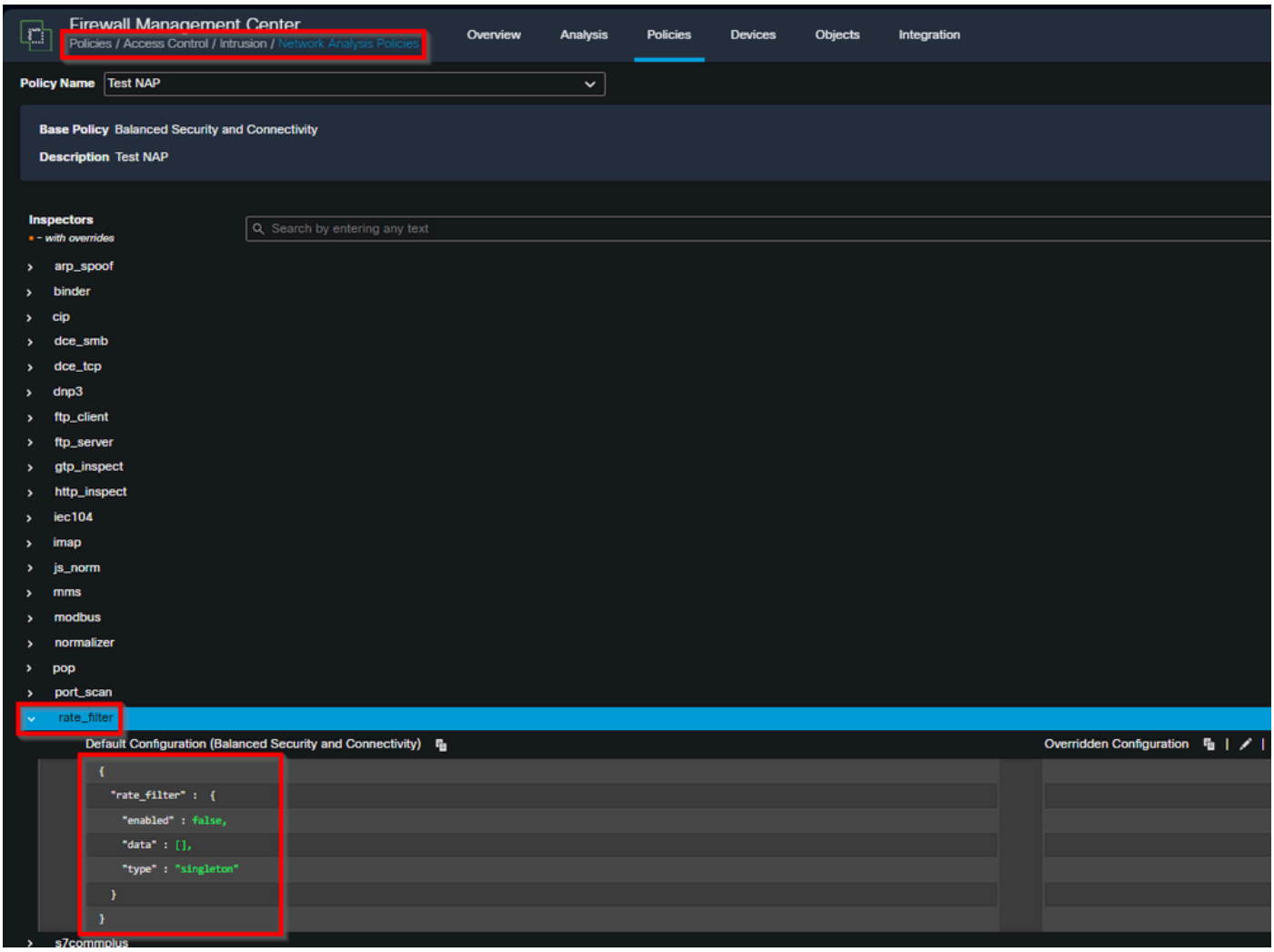
Opmerking: Het valt niet binnen het werkbereik van de TAC om specifieke waarden voor

---

deze regelfilters voor te stellen of aan te bevelen. Elke omgeving is anders en vereist een diepgaande analyse van verkeerspatronen en netwerkontwerp om de beste waarden voor deze filters te bepalen.

1: Navigeer naar het Snort 3 rate_filter

Deze filters worden geconfigureerd onder Beleid > Toegangscontrole: Inbraak > Netwerkanalysebeleid door te klikken op Versie 3 sorteren voor het NAP-beleid en vervolgens te klikken op de vervolgkeuzelijst rate_filter in het linkerdeelvenster.



inline_image_0.png

2: Begrijp de Snort 3 Rate Filter Rule Structure

Met de inspector rate_filter in Snort 3 kunt u regels definiëren die specifieke soorten verkeer controleren (zoals SYN-pakketten) en acties ondernemen (waarschuwen of laten vallen) wanneer een gedefinieerde drempel wordt overschreden. Deze regels kunnen gericht zijn op meerdere

subnetten.

Voorbeeld rate_filter configuratie voor meerdere subnetten:

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
        "count": 5,
        "gid": 135,
        "sid": 1,
        "new_action": "alert",
        "seconds": 10,
        "timeout": 15,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

Uitleg over de parameters:

- apply_to: Lijst van IP-adressen of subnetten waarop het filter van toepassing is (ondersteunt meerdere subnetten).
- aantal + seconden: drempelwaarde voor gebeurtenis (bijvoorbeeld 5 SYN-pakketten binnen 10 seconden).
- gid / sid: identificeert de Snort-gebeurtenis (zoals GID 135, SID 1 voor SYN-overstromingsdetectie).
- new_action: actie die moet worden ondernomen wanneer de drempelwaarde wordt overschreden (bijvoorbeeld alert, drop).
- time-out: duur voordat een nieuwe waarschuwing/actie voor dezelfde aandoening wordt geactiveerd.
- track: Trackingmodus (bijvoorbeeld by_src voor IP per bron, by_dst voor IP per bestemming).

3: Best practices voor het afstemmen van drempelwaarden en de implementatie van beleid

- Begin in de waarschuwingsmodus: Stel new_action in om waarschuwingen te geven en

gebruik conservatieve drempelwaarden (zoals hoger aantal en seconden) om fout-positieven te voorkomen.

- Basislijn netwerkverkeer: Monitor gegenereerde gebeurtenissen om te begrijpen hoe "normale" SYN-tarieven eruit zien voor uw omgeving en subnetten.
- Iteratief afstemmen van parameters: Aanpassen aantal, seconden en time-out op basis van waargenomen verkeerspatronen en operationele behoeften.
- Ga naar blokkeren: zodra u er zeker van bent dat drempelwaarden abnormaal gedrag nauwkeurig weergeven, wijzigt u new_action van alert naar drop of gelijkwaardig om aanvallen actief te blokkeren.
- Aparte filters indien nodig: Overweeg verschillende tarieflimieten voor verschillende segmenten of rollen (bijvoorbeeld servers versus gebruikerssubnetten) als verkeerspatronen variëren.
- Continue bewaking: Blijf alert en controleer op rate_filter-gebeurtenissen om snel afstemmingsproblemen of actieve bedreigingen te identificeren.

Oorzaak

None. De configuratie werd gevraagd voor proactieve beveiliging en als leidraad vanwege een eerder SYN-overstromingsincident.

Verwante inhoud

- Snort 3 Inspector Referentie: Snelheidsfilter
- Apparaatconfiguratiehandleiding Cisco Secure Firewall Management Center, 7.4: Aanvalspreventie op basis van snelheid
- 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.