Konfigurieren Sie die ratenbasierte Abwehr von Angriffen mit Snort 3 Rate Filter für sichere FTD

Problem

Der Schwerpunkt liegt auf der Strukturierung von Regeln für mehrere Subnetze, dem Verständnis von Best Practices für die Implementierung und der Bestimmung geeigneter Schwellenwerte (Zähler pro Sekunde) für Warnungen oder Blockierungen, insbesondere im Zusammenhang mit dem Hochwasserschutz von SYN.

Umwelt

- Cisco Secure Firewall Firepower mit FTD 7.4.2.4
- Firepower 2110 Hardwareplattform
- Verwaltet von FirePOWER Management Center (FMC) 7.6.2.1
- Snort 3 Intrusion Prevention System mit aktiviertem rate_filter inspector
- Mehrere interne Subnetze, die vor SYN-Überschwemmungen geschützt werden müssen
- Keine aktiven Fehler vorhanden; Konfigurationsanleitung für proaktive Abwehr

Auflösung

Diese Schritte beschreiben detailliert, wie Sie ratenbasierten Angriffsschutz mit dem rate_filter-Inspektor von Snort 3 auf Cisco Secure Firewall FTD konfigurieren und implementieren. Dazu gehören eine Erklärung der Regelstruktur für mehrere Subnetze und Best Practice-Empfehlungen. Diese Aktionen sollen helfen, Baselines für normalen Datenverkehr zu erstellen und eine effektive Erkennung oder Blockierung von SYN-Flood-Angriffen zu ermöglichen.

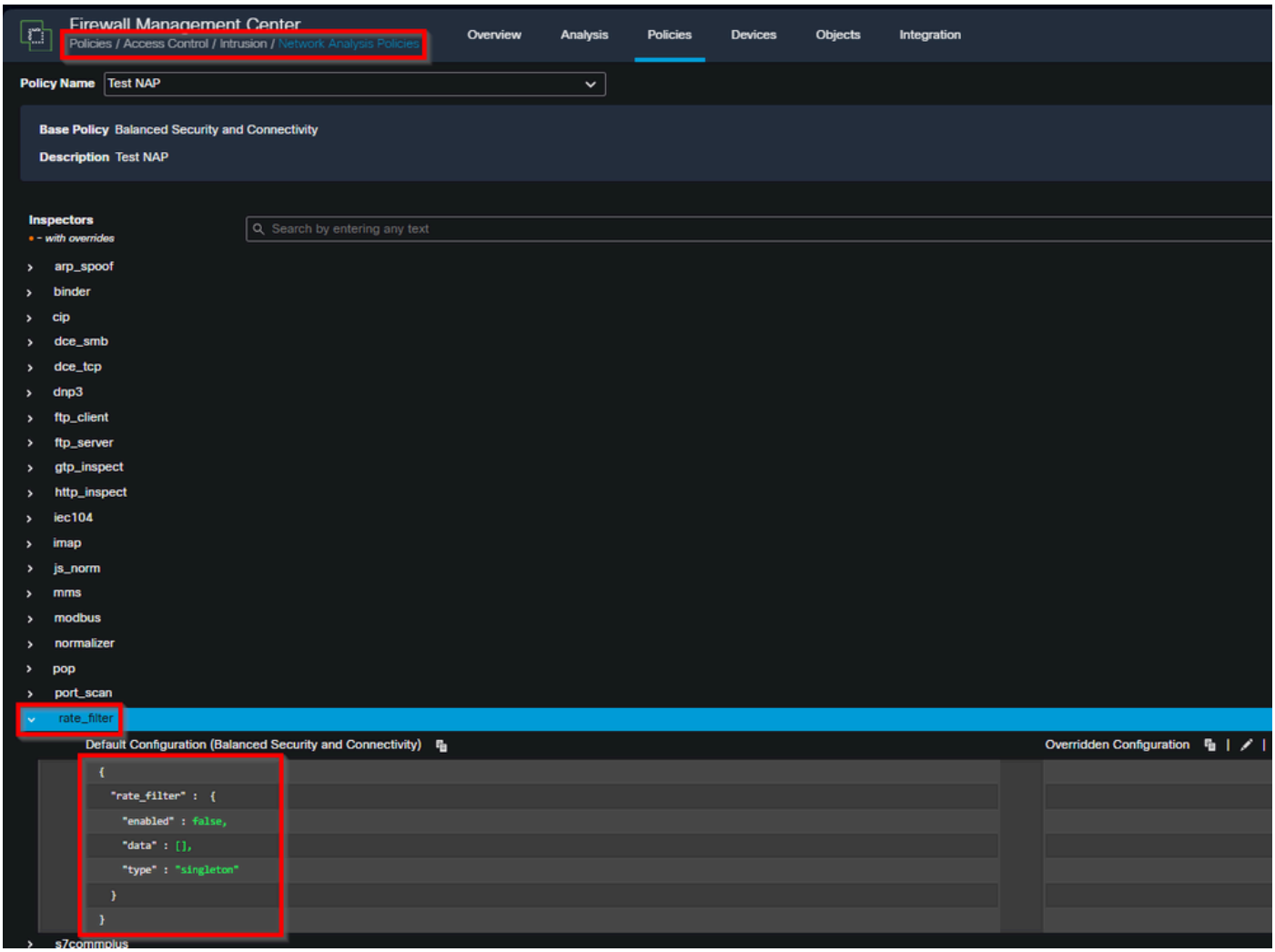
Anmerkung: Es liegt nicht im Aufgabenbereich des TAC, für diese Regelfilter bestimmte Werte vorzuschlagen oder zu empfehlen. Jede Umgebung ist anders und erfordert eine gründliche Analyse der Datenverkehrsmuster und des Netzwerkdesigns, um die besten

---

Werte für diese Filter zu bestimmen.

1: Navigieren Sie zu Snort 3 rate_filter

Diese Filter werden unter Richtlinien > Zugriffskontrolle: Eindringen > Richtlinien für die Netzwerkanalyse konfiguriert. Klicken Sie dazu auf Snort 3 Version für die NAP-Richtlinie und anschließend auf das Dropdown-Menü rate_filter im linken Bereich.



inline_image_0,png

2: Verstehen der Snort 3 Rate Filter-Regelstruktur

Mit dem rate_filter-Inspektor in Snort 3 können Sie Regeln definieren, die bestimmte Arten von Datenverkehr (z. B. SYN-Pakete) überwachen und Maßnahmen (Warnungen oder Löschungen) ergreifen, wenn ein definierter Grenzwert überschritten wird. Diese Regeln können auf mehrere Subnetze ausgerichtet werden.

Beispiel für rate_filter-Konfiguration für mehrere Subnetze:

```
{
  "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"
  }
}
```

Erläuterung der Parameter:

- apply_to: Liste der IP-Adressen oder Subnetze, auf die der Filter angewendet wird (unterstützt mehrere Subnetze).
- count + seconds: Schwellenwert für Ereignis (z. B. 5 SYN-Pakete innerhalb von 10 Sekunden).
- gid / sid: Identifiziert das Snort-Ereignis (z. B. ss GID 135, SID 1 für SYN-Flood-Erkennung).
- new_action: Aktion, die bei Überschreiten des Grenzwerts ausgeführt wird (z. B. alert, drop).
- timeout (Zeitüberschreitung): Zeitdauer, bis eine neue Warnung/Aktion für dieselbe Bedingung ausgelöst wird.
- track: Tracking-Modus (z. B. by_src für Pro-Source-IP, by_dst für Pro-Destination-IP).

3: Best Practices für die Anpassung von Schwellenwerten und die Bereitstellung von Richtlinien

- Im Warnmodus starten: Legen Sie new_action auf alert fest und verwenden Sie konservative Schwellenwerte (z. B. höhere Anzahl und Sekunden), um Fehlalarme zu vermeiden.
- Baseline-Netzwerkverkehr: Überwachen Sie die generierten Ereignisse, um zu ermitteln, wie die "normalen" SYN-Raten für Ihre Umgebung und Subnetze aussehen.
- Iterative Anpassung von Parametern: Passen Sie Zähler, Sekunden und Zeitüberschreitung

auf Basis der beobachteten Datenverkehrsmuster und betrieblichen Anforderungen an.

- Übergang zur Blockierung: Sobald Sie sicher sind, dass die Schwellenwerte anormales Verhalten genau widerspiegeln, ändern Sie new_action von alert in drop oder vergleichbar mit aktiv blockierten Angriffen.
- Separate Filter nach Bedarf: Unterschiedliche Durchsatzratenbeschränkungen für unterschiedliche Segmente oder Rollen (z. B. Server oder Benutzer-Subnetze) bei unterschiedlichen Datenverkehrsmustern berücksichtigen.
- Kontinuierliche Überwachung: Warn- und Überwachungsfunktionen für Rate_Filter-Ereignisse sorgen für eine schnelle Identifizierung von Optimierungsproblemen oder aktiven Bedrohungen.

Ursache

Keine. Die Konfiguration wurde aufgrund eines früheren SYN-Flood-Incident angefordert, um proaktive Sicherheit zu gewährleisten und als Hilfestellung zu dienen.

Verwandte Inhalte

- Snort 3 Inspector-Referenz: Ratenfilter
- Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.4: Ratenbasierter Schutz vor Angriffen
- 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.