Configuration de la prévention des attaques basée sur le taux avec le filtre de taux Snort 3 sur FTD sécurisé

Problème

L'accent est mis sur la manière de structurer les règles pour couvrir plusieurs sous-réseaux, la compréhension des meilleures pratiques de mise en oeuvre et la détermination des valeurs de seuil appropriées (nombres par seconde) pour les alertes ou le blocage, en particulier dans le contexte de la prévention des attaques SYN flood.

Environnement

- Cisco Secure Firewall Firepower exécutant FTD 7.4.2.4
- Plate-forme matérielle Firepower 2110
- Géré par Firepower Management Center (FMC) 7.6.2.1
- Système de prévention des intrusions Snort 3 avec l'inspecteur rate_filter activé
- Plusieurs sous-réseaux internes nécessitant une protection contre les inondations SYN
- Aucun défaut actif présent ; guide de configuration pour une défense proactive

Résolution

Ces étapes détaillent la configuration et la mise en oeuvre de la prévention d'attaque basée sur le débit à l'aide de l'inspecteur rate_filter de Snort 3 sur Cisco Secure Firewall FTD, y compris une explication de la structure des règles pour plusieurs sous-réseaux et des recommandations de meilleures pratiques. Ces actions sont destinées à aider à établir des lignes de base pour le trafic normal et à permettre une détection ou un blocage efficace des attaques SYN flood.

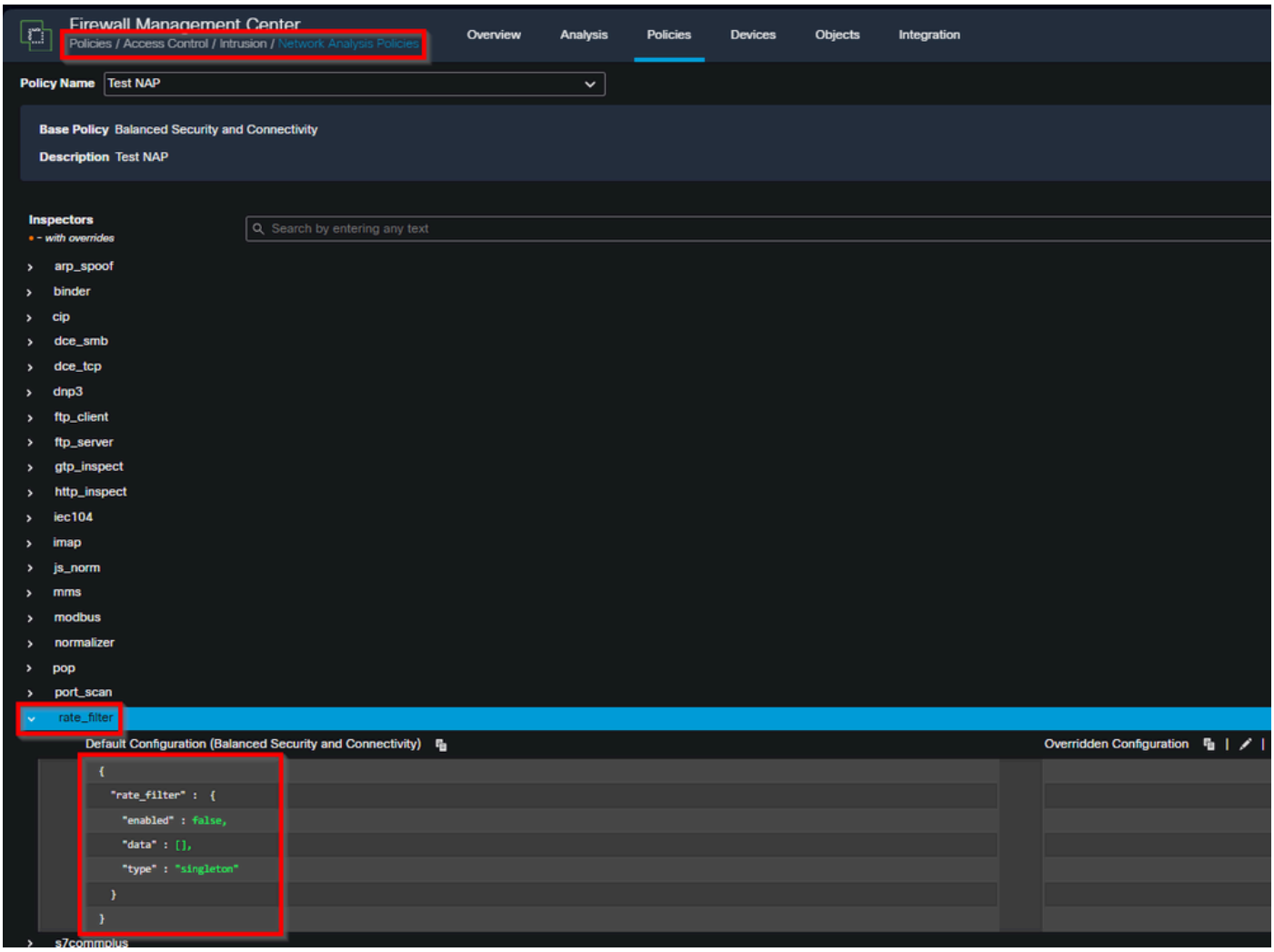
Remarque : Il n'est pas dans le cadre du travail du TAC de suggérer ou de recommander

---

des valeurs spécifiques pour ces filtres de règles. Chaque environnement est différent et nécessite une analyse approfondie des modèles de trafic et de la conception du réseau pour déterminer les meilleures valeurs pour ces filtres.

1 : Accédez à Snort 3 rate_filter

Ces filtres sont configurés sous Policies > Access Control: Intrusion > Network Analysis Policies en cliquant sur Snort 3 Version pour la stratégie NAP, puis en cliquant sur la liste déroulante rate_filter du panneau de gauche.



image_en_ligne_0.png

2 : Comprendre la structure de la règle de filtrage du taux de Snort 3

L'inspecteur rate_filter dans Snort 3 vous permet de définir des règles qui surveillent des types de trafic spécifiques (tels que des paquets SYN) et prennent des mesures (alerte ou abandon) lorsqu'un seuil défini est dépassé. Ces règles peuvent être ciblées sur plusieurs sous-réseaux.

Exemple de configuration de rate_filter pour plusieurs sous-réseaux :

```
{
  "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"
  }
}
```

Explication des paramètres :

- apply_to : liste des adresses IP ou des sous-réseaux auxquels le filtre s'applique (prend en charge plusieurs sous-réseaux).
- count + seconds : seuil pour l'événement (par exemple, 5 paquets SYN dans les 10 secondes).
- gid / sid : identifie l'événement Snort (tel que GID 135, SID 1 pour la détection d'inondation SYN).
- new_action : Action à entreprendre lorsque le seuil est dépassé (par exemple, alerte, abandon).
- timeout : durée avant qu'une nouvelle alerte/action ne soit déclenchée pour la même condition.
- track : mode de suivi (par exemple, by_src pour l'IP par source, by_dst pour l'IP par destination).

3 : Meilleures pratiques pour le réglage des seuils et le déploiement des politiques

- Commencer en mode alerte : définissez new_action sur alert et utilisez des seuils prudents (tels qu'un nombre plus élevé et des secondes) pour éviter les faux positifs.
- Trafic réseau de base : surveillez les événements générés pour comprendre à quoi ressemblent les taux SYN « normaux » pour votre environnement et vos sous-réseaux.

- Régler itérativement les paramètres : régler le nombre, les secondes et le délai d'attente en fonction des modèles de trafic observés et des besoins opérationnels.
- Passer au blocage : une fois que vous êtes sûr que les seuils reflètent précisément un comportement anormal, changez new_action de alert à drop ou équivalent à bloquer activement les attaques.
- Filtres distincts selon les besoins : tenez compte des différentes limites de débit pour les différents segments ou rôles (par exemple, serveurs et sous-réseaux d'utilisateurs) si les modèles de trafic varient.
- Surveillance continue : maintenez les alertes et la surveillance sur les événements rate_filter afin d'identifier rapidement les problèmes de réglage ou les menaces actives.

Motif

Aucune. La configuration a été demandée pour une sécurité proactive et comme guide en raison d'un précédent incident d'inondation SYN.

Autres informations utiles

- Snort 3 Inspector Référence : Filtre de débit
- Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.4 : Prévention des attaques basée sur le taux
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.