Configuración de la prevención de ataques basada en la velocidad con el filtro de velocidad Snort 3 en FTD seguro

Problema

El enfoque se centra en cómo estructurar las reglas para abarcar varias subredes, comprender las prácticas recomendadas para la implementación y determinar los valores de umbral adecuados (recuentos por segundo) para las alertas o los bloqueos, específicamente en el contexto de la prevención de ataques de inundación SYN.

Entorno

- Cisco Secure Firewall Firepower con FTD 7.4.2.4
- Plataforma de hardware Firepower 2110
- Administrado por Firepower Management Center (FMC) 7.6.2.1
- Sistema de prevención de intrusiones Snort 3 con el inspector rate_filter activado
- Varias subredes internas que requieren protección frente a inundaciones SYN
- No hay fallos activos; guía de configuración para la defensa proactiva

Resolución

Estos pasos detallan cómo configurar e implementar la prevención de ataques basada en la velocidad mediante el inspector rate_filter de Snort 3 en Cisco Secure Firewall FTD, incluida una explicación de la estructura de reglas para varias subredes y recomendaciones de prácticas recomendadas. Estas acciones están diseñadas para ayudar a establecer líneas de base para el tráfico normal y para habilitar la detección o el bloqueo efectivos de ataques de inundación SYN.

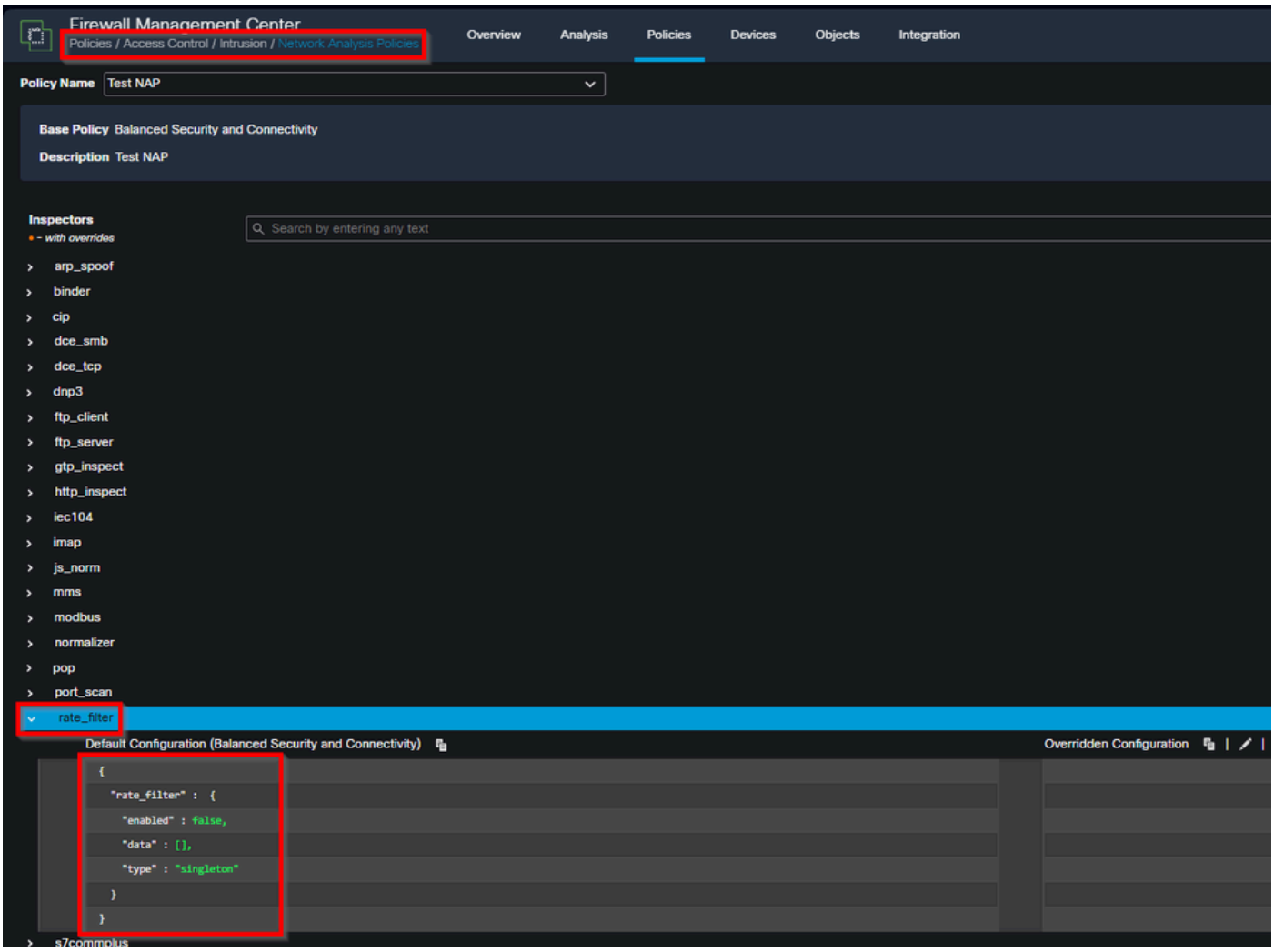
Nota: No está dentro del ámbito de trabajo del TAC sugerir o recomendar ningún valor

---

específico para estos filtros de regla. Cada entorno es diferente y requiere un análisis en profundidad de los patrones de tráfico y el diseño de red para determinar los mejores valores para estos filtros.

1: Vaya a Snort 3 rate_filter

Estos filtros se configuran en Políticas > Control de acceso: Intrusión > Políticas de análisis de red haciendo clic en Snort 3 Version para la política NAP y luego haciendo clic en el menú desplegable rate_filter del panel izquierdo.



inline_image_0.png

2: Comprensión de la estructura de reglas de filtro de velocidad de Snort 3

El inspector rate_filter de Snort 3 permite definir reglas que supervisan tipos específicos de tráfico (como paquetes SYN) y realizar acciones (alerta o descarte) cuando se excede un umbral definido. Estas reglas se pueden dirigir a varias subredes.

Ejemplo de configuración rate_filter para varias subredes:

```
{
  "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"
  }
}
```

Explicación de los parámetros:

- apply_to: Lista de direcciones IP o subredes a las que se aplica el filtro (soporta subredes múltiples).
- count + seconds: Umbral para el evento (por ejemplo, 5 paquetes SYN en 10 segundos).
- gid / sid: identifica el evento Snort (como GID 135, SID 1 para la detección de inundación SYN).
- new_action: Acción a tomar cuando se excede el umbral (por ejemplo, alerta, descartar).
- timeout: duración antes de que se desencadene una nueva alerta/acción para la misma condición.
- track: Modo de seguimiento (por ejemplo, by_src para IP por origen, by_dst para IP por destino).

3: Prácticas recomendadas para el ajuste de umbrales y la implementación de políticas

- Comenzar en modo de alerta: Defina new_action para alertar y utilice umbrales conservadores (como un mayor recuento y segundos) para evitar falsos positivos.
- Tráfico de red de referencia: supervise los eventos generados para comprender el aspecto de las velocidades SYN "normales" en su entorno y subredes.

- Ajuste iterativo de los parámetros: ajuste el recuento, los segundos y el tiempo de espera en función de los patrones de tráfico observados y las necesidades operativas.
- Pasar al bloqueo: Una vez que esté seguro de que los umbrales reflejan con precisión el comportamiento anormal, cambie new_action de alerta a drop o equivalente para bloquear activamente los ataques.
- Filtros separados según sea necesario: considere diferentes límites de velocidad para diferentes segmentos o roles (por ejemplo, servidores frente a subredes de usuario) si los patrones de tráfico varían.
- Supervisión continua: mantenga las alertas y la supervisión de los eventos rate_filter para identificar rápidamente los problemas de ajuste o las amenazas activas.

Causa

Ninguno. La configuración se solicitó para seguridad proactiva y como guía debido a un incidente de inundación SYN anterior.

Contenido relacionado

- Referencia del inspector de Snort 3: Filtro de velocidad
- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4: Prevención de ataques basada en la velocidad
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).