Configure a prevenção de ataques com base em taxa com o filtro de taxa Snort 3 no FTD seguro

Problema

O foco está em como estruturar regras para abranger várias sub-redes, compreender as melhores práticas de implementação e determinar os valores de limite apropriados (contagens por segundo) para alerta ou bloqueio, especificamente no contexto da prevenção de ataque de inundação SYN.

Ambiente

- Cisco Secure Firewall Firepower executando o FTD 7.4.2.4
- Plataforma de hardware Firepower 2110
- Gerenciado pelo Firepower Management Center (FMC) 7.6.2.1
- Sistema de prevenção de intrusão Snort 3 com o inspetor rate_filter habilitado
- Várias sub-redes internas que exigem proteção contra inundações SYN
- Ausência de defeitos ativos; orientação de configuração para defesa proativa

Resolução

Estas etapas detalham como configurar e implementar a prevenção de ataque baseada em taxa usando o inspetor rate_filter do Snort 3 no FTD do Cisco Secure Firewall, incluindo uma explicação da estrutura de regras para várias sub-redes e recomendações de práticas recomendadas. Essas ações têm o objetivo de ajudar a estabelecer linhas de base para o tráfego normal e permitir a detecção ou o bloqueio eficaz de ataques de inundação de SYN.

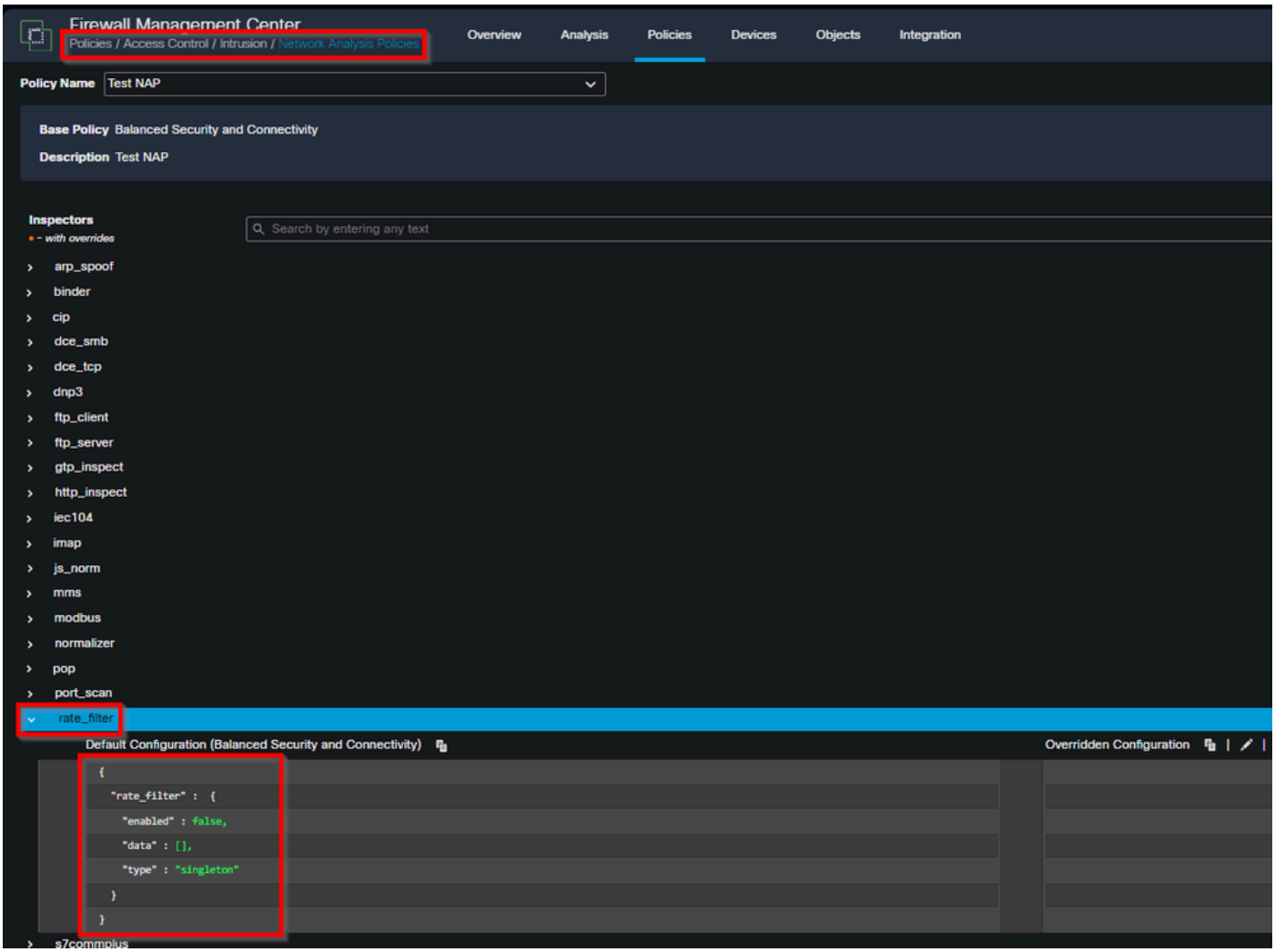
Note: Não faz parte do escopo de trabalho do TAC sugerir ou recomendar valores específicos para esses filtros de regras. Cada ambiente é diferente e requer uma análise detalhada dos padrões de tráfego e do projeto de rede para determinar os melhores

---

valores para esses filtros.

1: Navegue até a tabela rate_filter do Snort 3

Esses filtros são configurados em Policies > Access Control: Intrusion > Network Analysis Policies clicando em Snort 3 Version para a política NAP e clicando no menu suspenso rate_filter no painel esquerdo.



inline_image_0.png

2: Entender a estrutura da regra de filtro de taxa do Snort 3

O inspetor rate_filter no Snort 3 permite definir regras que monitoram tipos específicos de tráfego (como pacotes SYN) e tomam ações (alertar ou descartar) quando um limite definido é excedido. Essas regras podem ser direcionadas a várias sub-redes.

Exemplo de configuração de rate_filter para várias sub-redes:

```
{
  "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"
  }
}
```

Explicação dos parâmetros:

- apply_to: Lista de endereços IP ou sub-redes às quais o filtro se aplica (suporta várias sub-redes).
- count + seconds: Limite para o evento (por exemplo, 5 pacotes SYN em 10 segundos).
- gid / sid: identifica o evento Snort (como GID 135, SID 1 para detecção de inundação SYN).
- new_action: Ação a ser tomada quando o limite for excedido (por exemplo, alert, drop).
- timeout: A duração antes que um novo alerta/ação seja disparado para a mesma condição.
- track: Modo de rastreamento (por exemplo, by_src para IP por origem, by_dst para IP por destino).

3: Práticas recomendadas para ajuste de limites e implantação de políticas

- Comece no modo de alerta: Defina new_action como alert e use limites conservadores (como count mais alto e seconds) para evitar falsos positivos.
- Tráfego de rede de linha de base: monitore os eventos gerados para entender como são as taxas SYN "normais" para seu ambiente e sub-redes.
- Ajustar interativamente os parâmetros: Ajustar a contagem, os segundos e o tempo limite com base nos padrões de tráfego observados e nas necessidades operacionais.
- Mude para o bloqueio: Depois de ter certeza de que os limites refletem precisamente o comportamento anormal, altere new_action de alert para drop ou equivalente a bloquear ativamente os ataques.

- Filtros separados conforme necessário: considere limites de taxa diferentes para segmentos ou funções diferentes (por exemplo, servidores vs. sub-redes de usuário) se os padrões de tráfego variarem.
- Monitoramento contínuo: mantenha o alerta e o monitoramento em eventos rate_filter para identificar rapidamente problemas de ajuste ou ameaças ativas.

Causa

Nenhuma. A configuração foi solicitada para segurança proativa e como orientação devido a um incidente anterior de inundação de SYN.

Conteúdo relacionado

- Referência do inspetor do Snort 3: Filtro de Taxa
- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.4: Prevenção de ataques baseada em taxa
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.