Smart DDoS Filter

by Zevenet Team

Presentación Zevenet Team

Álvaro Cano

Luis Valencia

Laura García

Emilio Campos

Problemática

- Las reglas de protección no pueden ser genéricas para todas las aplicaciones, pretendemos aislar por flujo y aplicar distintas políticas de seguridad en ellos.

- La protección frente a atacantes es costosa en recursos (CPU + memoria)

Casos de uso

- Seguridad para dispositivos de red.
- Protección del canal de comunicación.
- Firewall perimetrales.
- Balanceadores de carga.

Propuesta

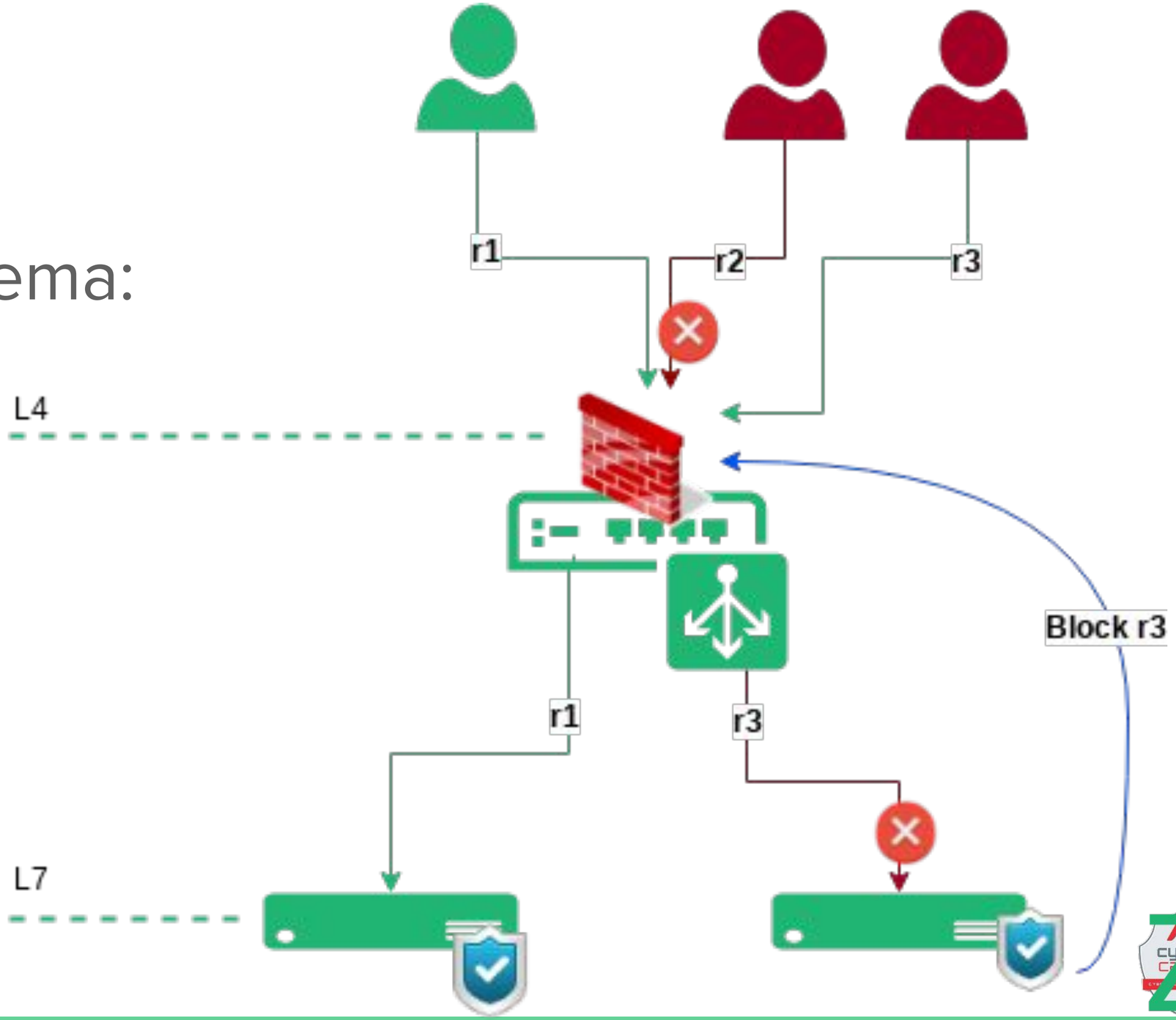
- Buscamos un sistema resiliente en seguridad, con detección temprana, mediante información dada por la detección en distintas capas L4 y L7.

- Otros sistemas se especializan en una determinada capa (por ejemplo antivirus), al unir diferentes niveles de protección conseguimos más eficiencia.

- Público objetivo: Todo sistema expuesto a internet.

Propuesta

Diagrama del sistema:



Implementación

- Desarrollo en lenguaje C de capacidades sobre nftlb para una primera capa de protección en nivel 4 de la capa OSI.

- Desarrollo de Lua scripting sobre modsecurity para reutilizar la información que proporciona por inspección de contenido a nivel de aplicación de la capa OSI.

- Crear interacción entre capas, usando lua. Seleccionamos nftables frente a iptables.

Expectativas

- Detección de ataques costosa, detectar más con menos recursos (CPU, memoria). Cuanto más temprano en el camino de datos podamos trabajar más eficientes seremos.

- Identificar ataques en diferentes capas del modelo OSI (L4 y L7) y reutilizar la información entre ellas y llevar a la etapa temprana del modelo de datos la información adquirida para ser más eficientes.