ReTEC

Revista Electrónica de Tecnología, Educación y Ciencia
ISSN: 2953-5654
http://retec.unsa.edu.ar
Universidad Nacional de Salta

Automatización de la seguridad en redes IPv6

Ernesto Sánchez[1 2], Henri Alves de Godoy[3], Daniel Arias Figueroa[1]

[1]C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada
[2]Facultad de Ingeniería – Universidad Católica de Salta
[3]Universidade Estadual de Campinas (UNICAMP, Brasil)
{ esanchez , daaf }@cidia.unsa.edu.ar

Revista Electrónica de Tecnología, Educación y Ciencia,

Volumen 1, Número 3, pág. 110-114, jun, 2026. ISSN: 2953-5654

Disponible en http://retec.unsa.edu.ar/

Automatización de la seguridad en redes IPv6

Ernesto Sánchez[1 2], Henri Alves de Godoy[3], Daniel Arias Figueroa[1]

[1]C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada
[2]Facultad de Ingeniería – Universidad Católica de Salta
[3]Universidade Estadual de Campinas (UNICAMP, Brasil)
{ esanchez , daaf }@cidia.unsa.edu.ar

Resumen: El presente trabajo aborda la automatización de la seguridad en redes IPv6 mediante la incorporación de mecanismos avanzados de telemetría de red y herramientas de configuración programable. En contraste con los enfoques tradicionales de monitoreo basados en sondeo, como SNMP y CLI, se propone un modelo proactivo sustentado en el streaming continuo de datos en tiempo real, utilizando protocolos modernos como gNMI, NETCONF/RESTCONF y JSON-RPC, bajo el marco conceptual definido por la RFC 9232. La investigación integra técnicas de automatización y análisis inteligente para mejorar la visibilidad, el control y la capacidad de respuesta ante incidentes de seguridad, particularmente en lo referente al manejo del tráfico ICMPv6 y los mecanismos de descubrimiento de vecinos (NDP). Asimismo, se incorpora el uso de Inteligencia Artificial como herramienta de apoyo en el desarrollo de scripts y configuraciones, optimizando los procesos de implementación y validación. El estudio se valida mediante un entorno experimental basado en el laboratorio Nokia SR Linux Streaming Telemetry Lab, donde se implementan mecanismos de descubrimiento automático de hosts, detección de dispositivos no autorizados y aplicación dinámica de listas de control de acceso (ACL). Los resultados evidencian una mejora significativa en la detección temprana de amenazas, la automatización de la mitigación de ataques y la interoperabilidad entre plataformas, consolidando a la telemetría como un componente clave en la evolución hacia redes IPv6 inteligentes, resilientes y autónomas.

Palabras clave: IPv6; telemetría de red; seguridad en redes; ICMPv6; Neighbor Discovery Protocol (NDP); automatización de redes; gNMI; JSON-RPC; NETCONF; modelos YANG; listas de control de acceso (ACL).

1. Introducción

Durante la reunión LACNIC 44, realizada en El Salvador, presentamos el trabajoo titulado Telemetria aplicada a la automatización de la seguridad en redes IPv6, resultado de una colaboración entre la Universidad Católica de Salta (Argentina) y la Universidade Estadual de Campinas (UNICAMP, Brasil).

El estudio demostró, de forma práctica, cómo el uso de protocolos de telemetría modernos e interfaces programables puede transformar la forma en que operamos y protegemos las redes IPv6, combinando visibilidad, automatización y seguridad. Con el creciente número de dispositivos, sensores IoT y flujos de datos, la visibilidad y el control de la red se han vuelto esenciales.

Durante mucho tiempo, la gestión de redes se realizaba con tecnologías tradicionales como SNMP y CLI, y a esto estábamos acostumbrados. Estos métodos carecen de escalabilidad, se

basan en formatos no estructurados y ofrecen una visibilidad limitada en tiempo real, lo que dificulta una reacción rápida ante incidentes de seguridad o fallos operativos.

En este contexto, la investigación presentada abordó el concepto de Telemetría de Red, un nuevo paradigma que reemplaza la recopilación reactiva de datos por un modelo proactivo y continuo, integrando automatización, seguridad e inteligencia operativa.

2. Transición del monitoreo clásico a la telemetría inteligente

Tradicionalmente, los administradores de red utilizaban el modelo de sondeo (polling), es decir, consultas periódicas a cada dispositivo, generalmente a través de SNMP, para recopilar información de estado. Además de generar sobrecarga, este proceso ofrece una visión fragmentada y diferida del estado de la red.

En vez de consultar a los dispositivos, la telemetría moderna transmite de manera continua sus métricas de desempeño, consumo de CPU, tráfico o eventos de seguridad en flujos de datos estructurados en tiempo real.

Este cambio se sustenta en protocolos de última generación, como:

- NETCONF y RESTCONF, basados en modelos YANG, que permiten configuraciones y consultas estandarizadas.
- gNMI (gRPC Network Management Interface), diseñada para un streaming continuo y eficiente.
- JSON-RPC, utilizado para llamadas a procedimientos remotos en formato JSON, ideal para la integración con sistemas de automatización y seguridad.

El uso combinado de estas tecnologías crea lo que la RFC 9232 denomina marco de telemetría de red, un conjunto de procesos y protocolos que ofrecen una visibilidad total de los diferentes planos de la red (datos, control y gestión).

Publicada por el IETF, la RFC 9232, Marco de Telemetría de Red, define la arquitectura y los principios fundamentales de la telemetría moderna. Propone la instrumentación en los diferentes planos de la red, como se describe a continuación:

- Plano de datos: monitorea el tráfico, las estadísticas de los paquetes, las pérdidas, las latencias y los flujos.
- Plano de control: acompaña los protocolos de enrutamiento y descubrimiento de vecinos (como ICMPv6 ND, OSPFv3 y BGP).
- Plano de gestión: recopila métricas de configuración, registros, listas de control de acceso (ACL), políticas y estados de seguridad.

El objetivo principal del marco es permitir la visibilidad, la automatización y la correlación inteligente de eventos para permitir la detección de anomalías, la optimización del desempeño, la verificación del cumplimiento de políticas y, lo más importante, la automatización de la respuesta a incidentes en tiempo real.

3. IA aplicada a la automatización de redes

Uno de los diferenciales de este proyecto es el uso de Inteligencia Artificial para respaldar el ciclo de desarrollo de la investigación. Aplicando ingeniería de prompts, se generaron scripts en Python y Scapy, además de configuraciones para las API gNMI y JSON-RPC, integradas en un entorno de control de procesos automatizado.

Esta metodología incluyó tres fases principales:

- Definición y diseño: identificación del problema y modelado de la arquitectura de la solución.
- Implementación asistida: colaboración humano-máquina en la creación de scripts, comandos e integración de los componentes.
- Validación y control: pruebas de seguridad, desempeño y robustez.

Es importante aclarar que, durante la investigación, la IA se utilizó únicamente como asistente técnico, sin reemplazar al investigador, sino simplemente aumentando la eficiencia y reduciendo el tiempo de implementación de las tareas.

4. Caso práctico: telemetría y seguridad en IPv6

El laboratorio de pruebas y simulación se desarrolló en la plataforma Nokia SR Linux Streaming Telemetry Lab, con topología virtualizada. Los nodos se integraron con gNMIc (cliente gRPC para recolección y suscripción a métricas) y visualización en Elasticsearch, Prometheus/Grafana, lo que permitió medir el comportamiento de la red y reaccionar a los eventos en forma dinámica. Gracias a este moderno marco de telemetría, pudimos resolver algunas de las necesidades de investigación junto con algunos de los desafíos que teníamos, por ejemplo:

- Descubrir automáticamente los hosts en redes IPv6.
- Detectar los dispositivos desconocidos o no autorizados.
- Aplicar ACL dinámicas en tiempo real para mitigar ataques basados en descubrimiento de vecinos ICMPv6.
- Suscribirse a métricas de tráfico y desempeño en interfaces, ACL y CPU vía streaming gNMI.

A continuación mostramos parte de un ejemplo de binding generado automáticamente entre una dirección MAC e IPv6:

```
{
  "mac": "aa:c1:ab:55:20:5a",
  "interface": "ethernet-1/2.0",
  "ipv6_link_local": "fe80::a8c1:abff:fe55:205a",
  "ipv6_global": "2001:db8:20:0:a8c1:abff:fe55:205a",
  "timestamp": "2025-06-10T01:28:39.773935"
}
```

Con base en esta información, el sistema:

Envía los bindings válidos vía JSON-RPC a Elasticsearch para su serialización e indexación, donde luego se convierten en una fuente de datos para su visualización en Grafana.

Aplica políticas dinámicas vía JSON-RPC/YANG para permitir o bloquear el tráfico ICMPv6 de acuerdo con reglas predefinidas.

```
set acl acl-filter {iface} type ipv6 entry 10 match ipv6 next-header
icmp6 source-ip prefix {ipv6_link_local}/128
set acl acl-filter {iface} type ipv6 entry 10 action accept
set acl acl-filter {iface} type ipv6 entry 11 match ipv6 next-header
icmp6 source-ip prefix {ipv6_global}/128
set acl acl-filter {iface} type ipv6 entry 11 action accept
```

Estas métricas se recopilan vía gNMI stream-mode sample cada 5 segundos y se exportan en formato Prometheus, lo que permite su visualización instantánea en Grafana.

5. Resultados

La investigación demostró que una telemetría moderna basada en gNMI y JSON-RPC no solo monitorea, sino que también integra seguridad, automatización y análisis operativo en un único flujo de datos. Por lo tanto, se está consolidando como un elemento estratégico para la confiabilidad y la seguridad de las redes IPv6, permitiendo que instituciones académicas, proveedores de servicios de Internet y empresas avancen hacia la operación de redes inteligentes, resilientes y autónomas.

Finalmente, las pruebas realizadas demostraron avances significativos:

- Detección anticipada de amenazas: la telemetría basada en streaming detecta cambios y anomalías en el tráfico de forma prácticamente instantánea.
- Automatización de la mitigación: las ACL se aplican de forma dinámica, reduciendo así la intervención humana y el tiempo de respuesta.
- Interoperabilidad real: el uso de modelos YANG abiertos (OpenConfig) elimina la dependencia de los fabricantes y simplifica la integración.

Referencias

1. RFC 9232 — Framework for Network Telemetry
2. OpenConfig / gNMI — https://gnmic.openconfig.net
3. Nokia SR Linux Telemetry Lab — https://github.com/srl-labs/srl-telemetry-lab
4. Documentación YANG Nokia — https://yang.srlinux.dev
5. Proyecto Telemetría IPv6 — https://github.com/ernestosv73/telemetria-ipv6
6. Video demostrativo — https://www.youtube.com/watch?v=u7ans7c86NA