Webinar
Seguridad en IPv6

Henri Alves de Godoy

Universidade Estadual de Campinas

Ernesto Sánchez

Universidad Católica de Salta - Universidad Nacional de Salta

Agenda - Parte 1

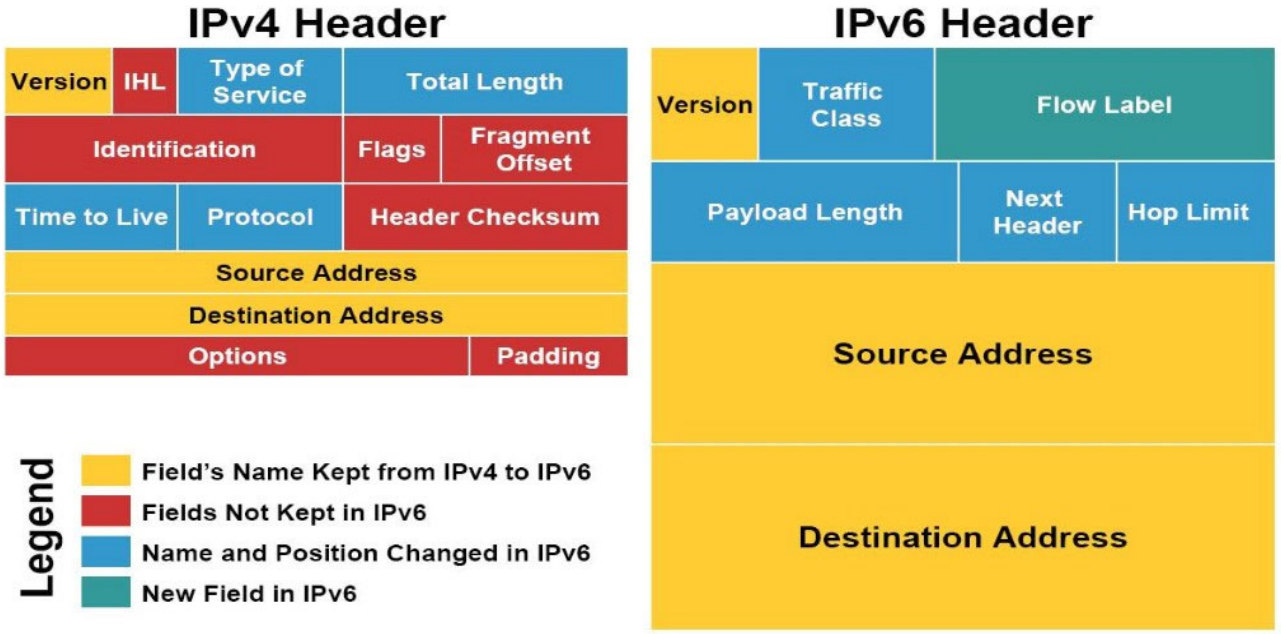
- Endereçamento no IPv6
- Criptografia e IPSec
- Firewalls e ACL
- Varredura e Monitoramento
- Boas Práticas com IPv6

O IPv6 e sua Necessidade

- Em LACNIC 36/2021, **Vint Cerf** comentou o erro de prever que 4,2 bilhões de endereços IPv4 seria suficiente para atender todo o mundo. (4 bilhões de pessoas na época, 2 mil computadores conectados).
- Um grande arrependimento não ter pensando no princípio sobre criptografia, mas não era possível na época.
- A princípio tinha um único objetivo. Era “apenas” aumentar o campo de IP para maior que 32 bits.
- 4,2 bilhões de endereços únicos para 340 undecilhões de endereços possíveis.

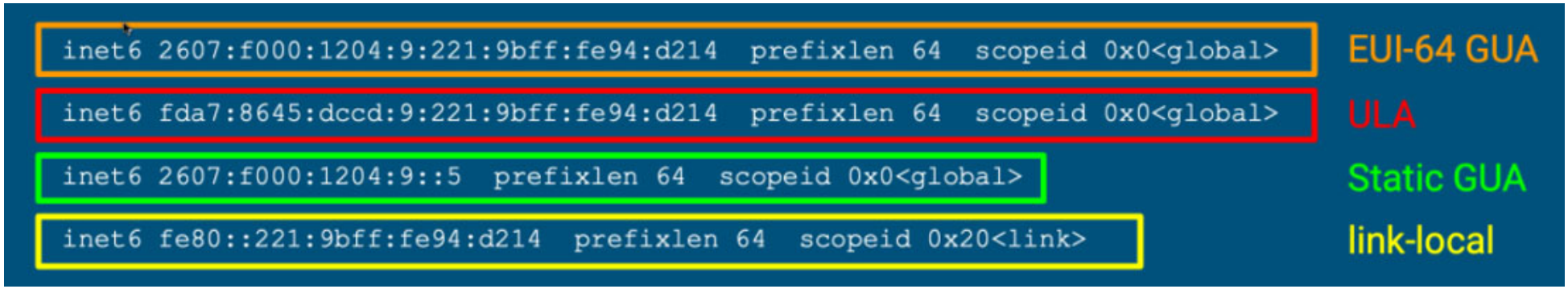
Comparação: Cabeçalhos IPv4 vs. IPv6

- RFC 2460 - IPv6 Specification – Dez. 1998
- RFC 8200 - Internet Standards IPv6 – Jul. 2017



Tipos de Endereços IPv6

- É normal ter vários endereços em uma interface, que se alteram com o tempo.
- Temos tipos de endereços de IPv6 e formas de entrega: SLAAC ou DHCPv6.
- Respeita a privacidade do usuário:
  - Antes: SLAAC RFC 2462 – EUI-64
  - Agora: SLAAC RFC 8981 (02/21). Randon Interface ID que muda com o tempo (aleatório) e não são reutilizados.



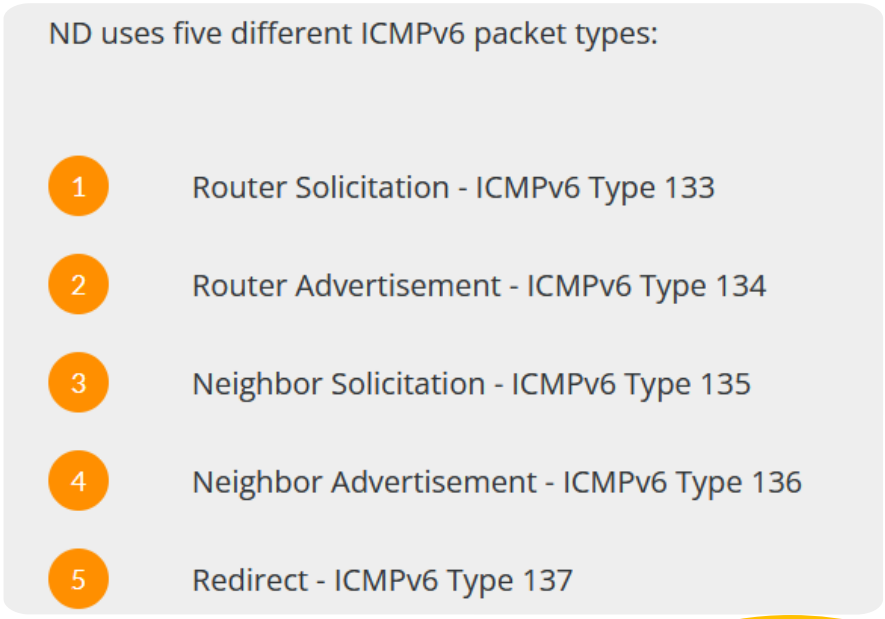
NAT e IPv6: realidades sobre segurança

- Um dos equívocos mais comuns em relação à segurança IPv6 é dizer que a falta do NAT torna o IPv6 menos seguro.
- O NAT44 é frequentemente visto como um recurso de segurança em redes IPv4.
- O uso de endereços globais no IPv6 e a restauração da conectividade de ponta-ponta causa uma surpresa em muita gente.
- Os firewalls podem facilmente fornecer proteção equivalente e melhor do que o NAT sem quebrar a conectividade de ponta-ponta.

Firewall no IPv6

- Por vezes, uma boa prática em IPv4 é o oposto redes com IPv6.
- Não é simplesmente copiar as regras. Exemplo:
  - Prática comum é bloquear em redes IPv4 o protocolo ICMP. Já em uma rede IPv6 isso não é possível (ICMPv6).

Recommendations for Filtering ICMPv6 Messages in Firewalls (RFC 4890).



Fonte: RIPE NCC

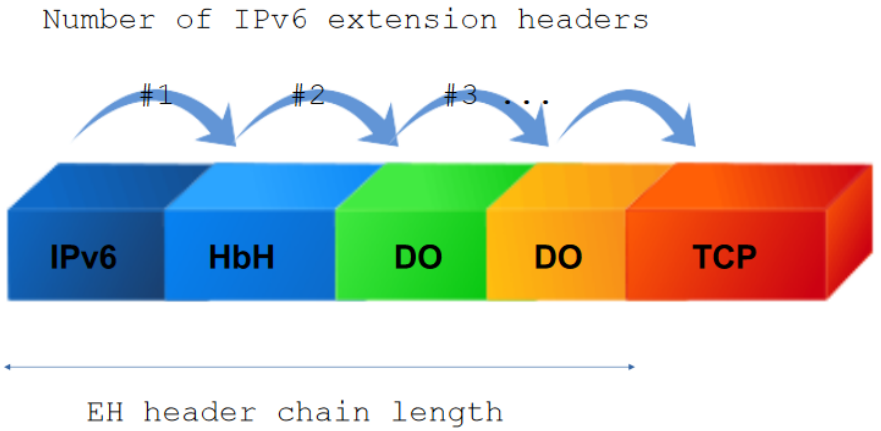
Criptografia no IPv6: O Papel do IPSec

- O IPv6 possui IPSec integrado como parte do protocolo e não é um complemento como no IPv4. No entanto, isso não significa que está ativado por padrão, apenas significa que há uma sobrecarga (teoricamente) menor na pilha de rede.

- IPSec foi considerado ao projetar o IPv6, no sentido de que, ao contrário do IPv4, o IPSec (quando usado) faz parte do cabeçalho.

Cabeçalhos de Extensão IPv6

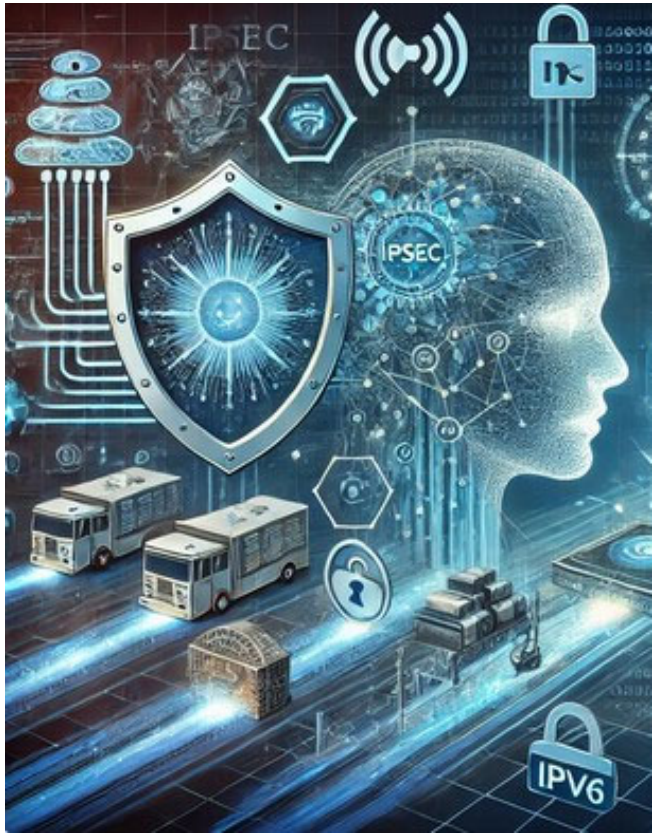
- Hop-by-Hop Options
- Routing
- Fragment
- Destination Options
- Authentication
- Encapsulating Security Payload



Fonte: https://www.lacnic.net/innovaportal/file/5591/1/fgont-lacnog2021-ipv6-ehs-packet-drops-lightning-talk.pdf

O estado atual do IPSec

- Havia uma expectativa que com o IPv6, o IPSec se tornaria mais utilizado. Por motivos comerciais, a criptografia se tornou mais popular com os certificados TLS para proteger a aplicação.
- Mas, temos casos do uso IPSec com IPv6 para proteger o tráfego de Data Centers, permitindo a desativação dos concentradores VPN existentes.
- Uma nova oportunidade para o IPSec tem surgido com o aumento da Inteligência Artificial (IA).
- Processamento de grandes volumes de dados confidenciais e sistemas de controle de infraestrutura crítica.



Varredura no IPv6: Desafios e Técnicas

- No IPv6 a varredura é um pouco mais difícil do que o IPv4. Mesmo assim temos ferramentas que começaram a varrer o espaço de endereçamento IPv6.
- A dificuldade depende do tipo de endereço que está atribuído e onde a ferramenta de scanner está localizada.
- Se os endereços IPv6 da rede foram atribuídos utilizando uma política conhecida, a varredura se tornará muito mais fácil. Por exemplo, algumas organizações numeram seus hosts sequencialmente.
- Alguns baseiam sua estrutura de endereços IPv6 em endereços IPv4 ou em portas de serviços.

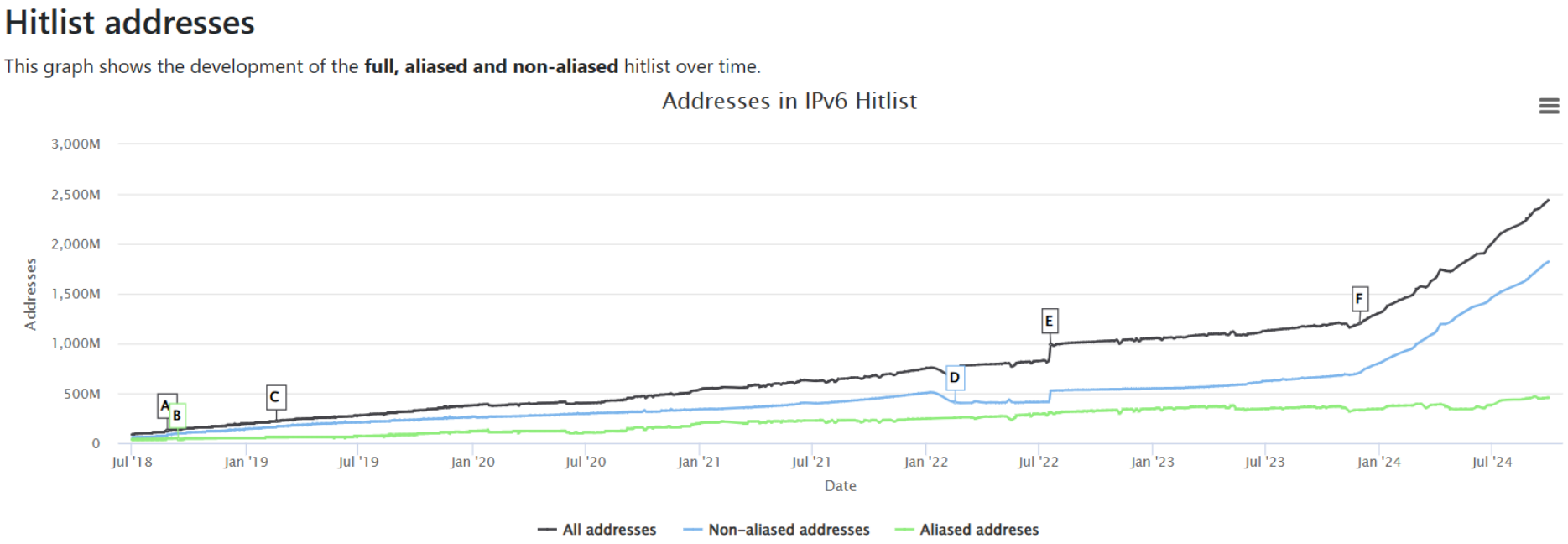
Estratégias de Varredura IPv6

No entanto, servidores, roteadores e outros sistemas de infraestrutura tendem a empregar configuração manual e normalmente resultam em endereços previsíveis que podem ser facilmente descobertos por meio de varreduras de endereços IPv6.

- Sondas multicast - Um endereço multicast especial é o ff02::1
- Consultas DNS multicast (mDNS).
- Transferências de zona DNS.
- Mapeamentos reversos de DNS.

IPv6 Hitlist Service

- https://ipv6hitlist.github.io/



Scanners IPv6

- Alguns scanners não usam um único endereço de origem IPv6 de 128 bits para enviar suas sondas de varredura. Em vez disso, eles geram seu tráfego de inúmeros endereços de origem em prefixos como /64, /48 ou até mesmo /32.
- A varredura é uma das primeiras coisas que pessoas mal intencionadas fazem a fim de encontrar vulnerabilidade ou explorar sistemas.

			scan sources		
rank	AS type	packets	/48s	/64s	/128s
#1	Datacenter (CN)	839M (39.2%)	1	1	1
#2	Datacenter (CN)	744M (34.8%)	1	1	5
#3	Cybersecurity (US)	275M (12.9%)	1	1	12
#4	Cloud (US/global)	78M (3.7%)	2	2	512
#5	Cloud (DE)	48M (2.3%)	3	59	59
#6	Cloud (US/global)	45M (2.1%)	10	15	205
#7	Cloud (US/global)	39M (1.8%)	9	9	123
#8	Cloud (CN)	30M (1.4%)	5	5	53
#9	Transit (global)	11M (0.5%)	1	2	956
#10	Cloud (CN)	10M (0.5%)	1	1	7
#11	Cloud (US/global)	4.7M (0.2%)	1	1	353
#12	Datacenter (CN)	3.1M (0.1%)	9	12	19
#13	ISP (VN)	2.5M (0.1%)	1	1	1
#14	Datacenter (CN)	1.6M (≤ 0.1%)	1	1	2
#15	Research (DE)	1.1M (≤ 0.1%)	1	1	1
#16	ISP (RU)	0.9M (≤ 0.1%)	1	1	2
#17	University (DE)	0.8M (≤ 0.1%)	1	1	2
#18	Cloud/Transit (DE)	0.6M (≤ 0.1%)	1,092	1,057	1,057
#19	ISP (RU)	0.6M (≤ 0.1%)	1	1	1
#20	University (DE)	0.5M (≤ 0.1%)	1	1	1

Fonte: ACM Internet Measurement Conference October 2022.

Impactos dos bloqueios de scanners IPv6

- Em situações operacionais, se a detecção de varredura levar à uma lista de bloqueios, a agregação grosseira também bloqueará o tráfego de fontes legítimas. (AWS, Google Cloud, Azure).
- Como escolher esse ajuste fino ainda é um desafio.
- É suficiente uma única ACL /128 ou devemos escalar para /64 ou /56, /52, /48 ?
- Ainda, se endereços temporários forem empregados, os firewalls de host e de rede geralmente devem ser configurados de modo que as comunicações de saída sejam permitidas de qualquer endereço, mas as comunicações de entrada sejam permitidas apenas para endereços estáveis.

Monitoramento Contínuo em Redes IPv6

Devemos monitorar sempre os padrões de tráfego de saída da rede e nunca ignorar o IPv6.

- Túneis automáticos.
- Exfiltracao de Dados.
- Anúncios RA não autorizados.

Artigo em Blog LACNIC - **Os riscos de ignorar o IPv6 na sua rede**

https://blog.lacnic.net/pt-br/os-riscos-de-ignorar-o-ipv6-na-sua-rede/

Segurança em Ambientes Dual-Stack IPv4/IPv6

- Do ponto de vista da segurança, é importante que as mesmas políticas de segurança sejam aplicadas para IPv4 e IPv6.
- Há uma tendência de que as políticas de filtragem de pacotes IPv6 são “mais fracas” do que as tradicionalmente IPv4. A falta momentânea no roteamento do tráfego IPv4, pode priorizar o fluxo de dados em IPv6.
- Em cenários onde endereços temporários são empregados, podem ser difíceis correlacionar os endereços de rede. É necessário manter registros (logs) centralizado de quais endereços foram empregados por qual host.
- Necessidade de adequar as ferramentas de monitoramento, NetFlows, Firewalls, Detecção de Intrusão (Suricata), SIEM.

Boas Práticas de Segurança

Criar Laboratórios e Simulações com IPv6 e IPv4.

Definir uma política de endereçamento IPv6 (SLAAC/DHCPv6). Escolher o método que ofereça mais controle.

Realizar pen tests para validar firewalls e ACLs. Ajustar regras conforme os resultados.

Priorizar o IPv6: Tratar o IPv6 corretamente em vez de desativá-lo.

Configurar as redes como IPv6-Only: Eliminar as vulnerabilidades associadas ao IPv4. Simplificar a gestão de segurança.

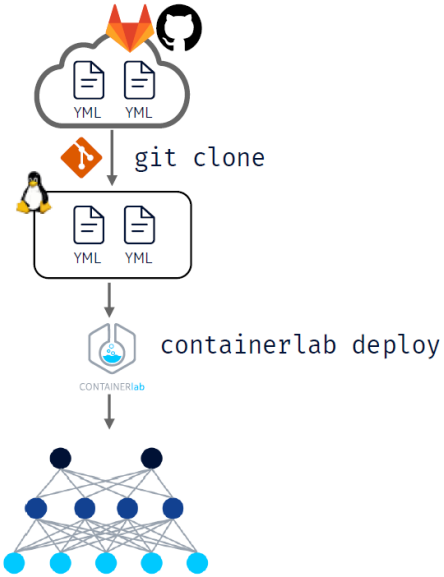
Agenda - Parte 2

- Containerlab: Virtualización de redes basada en contenedores.
- Topología Seguridad IPv6.
- Configuración de reglas de alerta personalizadas en IDS Suricata.
- Mitigación de vulnerabilidades. Configuración de ACLs en NOKIA SRL Linux.

Containerlab: Free and opensource networking lab environment for the modern age

Roman Dudin

CONTAINERlab



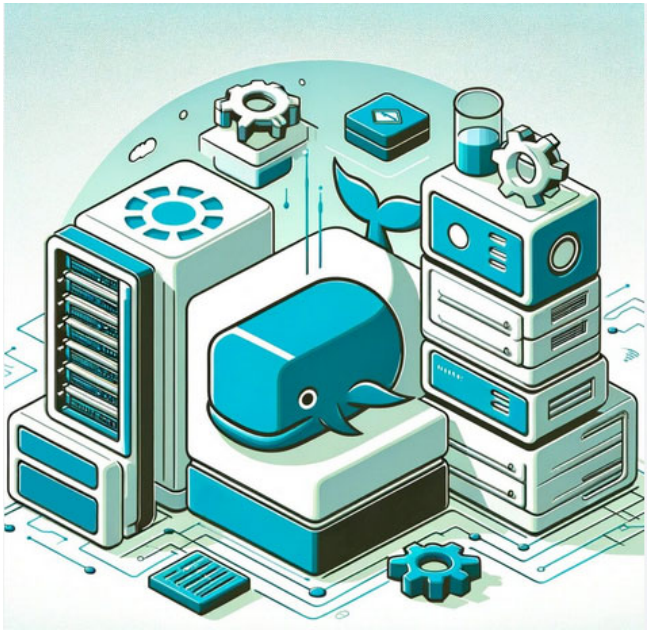
Git Friendly. Formato declarativo de topologias en archivos .yml.

Virtualización de NOS basada en contenedores. Nokia SR Linux, Arista cEOS, Juniper cRPD, Cumulus VX, FRR y otros.

Integración con Edgeshark para la captura de tráfico de red entre contenedores

NOKIA

Requisitos instalación entorno de pruebas



Ubuntu Server 22.04 con Docker CE. IPv6 no debe estar desactivado en el Kernel

Descarga e instalación de Containerlab: https://containerlab.dev/install/

```
bash -c "$(curl -sL https://get.containerlab.dev)“
```

Instalación y deploy de Edgeshark:

```
curl -sL \
https://github.com/siemens/edgeshark/raw/main/deploym
ents/wget/docker-compose.yaml \ |
DOCKER_DEFAULT_PLATFORM= docker compose -f - up -d
```

Clonar la topologia desde el repositorio Git:

```
git clone https://github.com/ernestosv73/ids
```

Deploy de topología y conexión a los nodos

```
+---+------------------+-------------+-----------------------------------------------------------------+-----
---------+---------+----------------+---------------------+
| # |       Name       | Container ID |                          Image                                  |
Kind      |  State  |  IPv4 Address  |     IPv6 Address    |
+---+------------------+-------------+-----------------------------------------------------------------+-----
---------+---------+----------------+---------------------+
| 1 | clab-ids-PC1     | 7a7273ca3b0d | docker.io/esanchezv/kaliipv6v2.1:latest                         | linu
x         | running | 172.20.20.2/24 | 2001:172:20:20::4/64 |
| 2 | clab-ids-PC2     | 1c211f687255 | docker.io/esanchezv/kaliipv6v2.1:latest                         | linu
x         | running | 172.20.20.10/24 | 2001:172:20:20::a/64 |
| 3 | clab-ids-PC3     | 6b6c1548e752 | esanchezv/exfil:latest                                          | linu
x         | running | 172.20.20.6/24 | 2001:172:20:20::8/64 |
| 4 | clab-ids-PC4     | c893a381aaf1 | esanchezv/exfil:latest                                          | linu
x         | running | 172.20.20.5/24 | 2001:172:20:20::7/64 |
| 5 | clab-ids-elastic | 845994cefd35 | docker.elastic.co/elasticsearch/elasticsearch:7.17.7            | linu
x         | running | 172.20.20.9/24 | 2001:172:20:20::2/64 |
| 6 | clab-ids-kibana  | 2eec1cf144e8 | docker.elastic.co/kibana/kibana:7.17.7                          | linu
x         | running | 172.20.20.7/24 | 2001:172:20:20::3/64 |
| 7 | clab-ids-srl1    | ca3b9f7450b3 | ghcr.io/nokia/srlinux:23.10.1                                   | noki
a_srlinux | running | 172.20.20.8/24 | 2001:172:20:20::9/64 |
| 8 | clab-ids-srl2    | 18bf03de73ca | ghcr.io/nokia/srlinux:23.10.1                                   | noki
a_srlinux | running | 172.20.20.3/24 | 2001:172:20:20::5/64 |
| 9 | clab-ids-suricata | 5b8166164e70 | docker.esanchezv/suricatafilebeatv1:v1                          | linu
x         | running | 172.20.20.4/24 | 2001:172:20:20::6/64 |
+---+------------------+-------------+-----------------------------------------------------------------+-----
---------+---------+----------------+---------------------+
root@uclab:/home/ernesto/ids#
```

CONTAINERlab

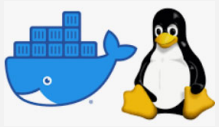
Ejecutar el comando

```
clab deploy -t ids.yml
```

SR Linux

Conexión al nodo Nokia SRL Linux

```
ssh admin@clab-ids-srl1
Password: NokiaSrl1!
```



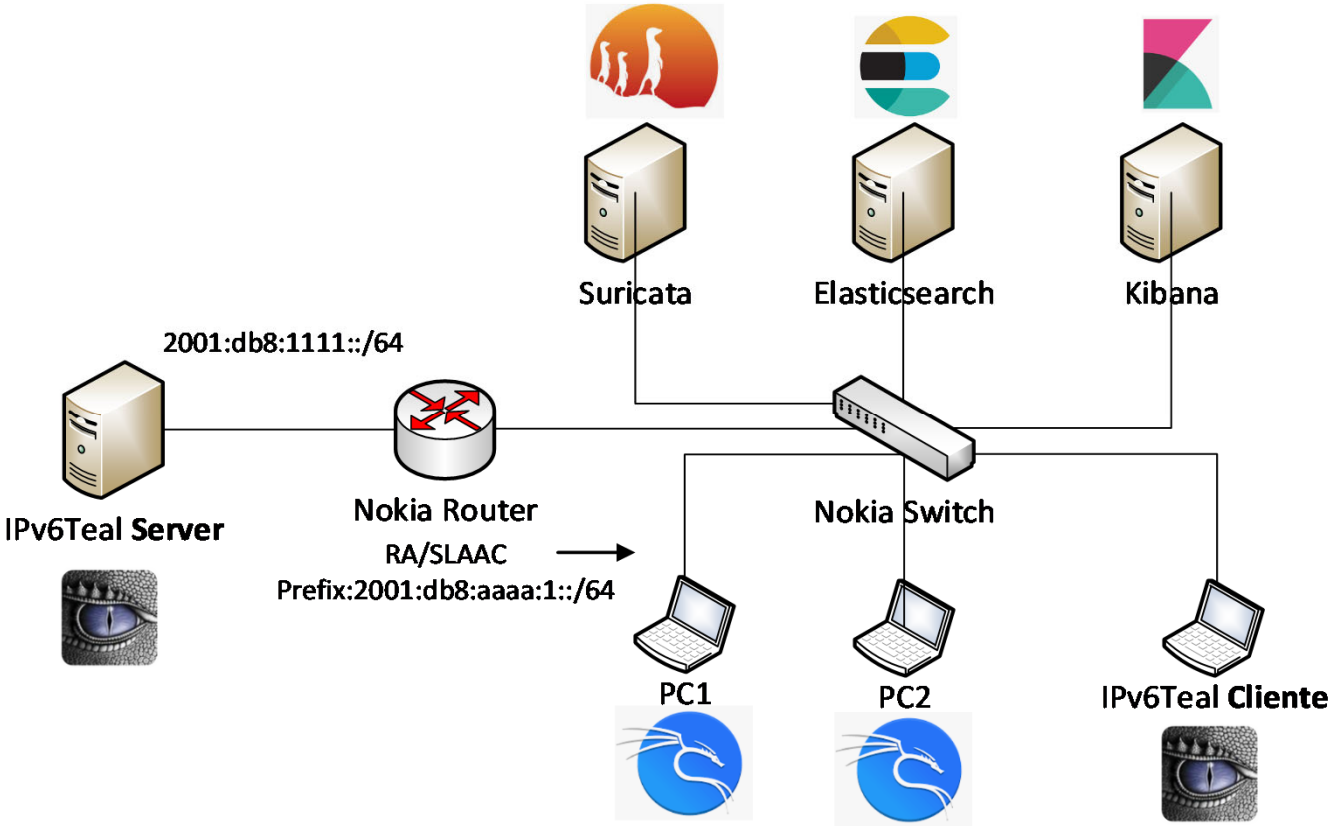
Conexión a los nodos Linux

```
docker exec -it clab-ids-nodo /bin/bash
```

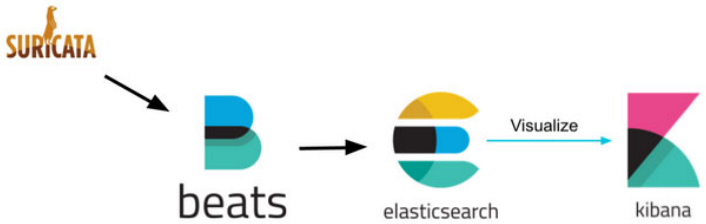
Captura de tráfico desde navegador SO host accedemos a: `http://ip-Ubuntu-server:5001`

Topología Seguridad IPv6 Containerlab

La topología de red configurada aborda el análisis de seguridad para el proceso de autoconfiguración de direcciones IPv6 sin estado, (SLAAC). RFC 4862, RFC 7527, RFC 4941.



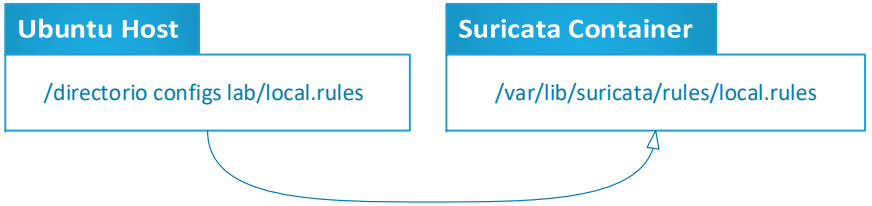
Configuración NIDS



Iniciar servicios en nodo Suricata:

```
root@suricata:/# /etc/init.d/suricata start
root@suricata:/# filebeat setup
root@suricata:/# /etc/init.d/filebeat start
```

File binding local.rules:



Desde navegador Ubuntu host, accedemos al panel de control Kibana:

`http://ip-Ubuntu-server:5601`

Configuración de reglas de alerta personalizadas en IDS Suricata

Tres componentes principales

Action

- Alert (IDS)
- Pass (IDS)
- Drop (IPS)
- Reject (IPS)

Header

- Prot: TCP, UDP, ICMP, etc.
- Source.
- Source Port.
- Direction.
- Destination.
- Dst Port.

(Options)

Condiciones que deben cumplirse para que se active la regla. Se basa en una lista de palabras claves. Estas palabras clave pueden incluir detalles como el contenido del paquete, el tamaño, etc.

Escenario 1: Escaneo en una Red LAN IPv6 con IPv6toolkit: `scan6 -i eth1 -L`
En base al análisis de tráfico de red se define la regla:

```
alert ipv6 any any -> ff02::1 any (msg:"ICMPv6 SCAN Local Net"; ip_proto:58;
itype:128; icode:0; classtype:policy-violation; sid:1000005; rev:1;)
```

Fuentes: https://www.kali.org/tools/ipv6toolkit/#scan6
https://docs.suricata.io/en/latest/rules/header-keywords.html

Configuración de reglas de alerta personalizadas en IDS Suricata

Ataques comunes con herramientas THC IPv6 y IPv6toolkit

Escenario 2: Ataque DoS mediante inundación de mensajes RA: `atk6-flood_router26 eth1`

Keyword: **threshold** permite controlar la frecuencia de las alertas. Tres modos (threshold, limit y both)
Type threshold: Permite establecer un umbral mínimo para una regla antes de generar un alerta.
Type limit: Su utilización asegura que no ocurra una inundación de alertas.
Type both: Combinación de las dos anteriores.

```
alert ipv6 any any -> any any (msg:"ICMPv6 Flood RA"; ip_proto:58; itype:134;
icode:0; threshold: type both, track by_dst, count 100, seconds 5;
classtype:policy-violation; sid:1000003; rev:1;)
```

Esta regla genera un alerta si desde cualquier fuente se envían 100 mensajes RA o más en un periodo de tiempo de 5 segundos.

Fuentes: https://docs.suricata.io/en/suricata-6.0.0/rules/thresholding.html?highlight=threshold%20type%20both
https://www.kali.org/tools/thc-ipv6/#atk6-flood_router26

Configuración de reglas de alerta personalizadas en IDS Suricata

Ataques comunes con herramientas THC IPv6 y IPv6toolkit

Escenario 3: Ataque DoS mediante mensaje RA con campo router lifetime = 0: `atk6-kill_router6 eth1 '*'`

Secuencia del ataque:

1. El atacante captura tráfico de red a la espera de un mensaje RA legítimo.
2. Con la información capturada, realiza suplantación de identidad utilizando la dirección link local del router y envía mensaje RA con campo router lifetime = 0.

Configuración de regla: Debemos "mirar" valores en campos de encabezado ICMPv6. Keywords: icmpv6.hdr, content, offset y depth. content:"|00 00|"; offset:6; depth:2; indica valor 0 para el campo router lifetime

```
alert ipv6 any any -> ff02::1 any (msg:"ICMPv6 Kill Router6"; ip_proto:58;
itype:134; icode:0; icmpv6.hdr; content:"|00 00|"; offset:6; depth:2;
classtype:policy-violation; sid:1000006; rev:1;)
```

Fuentes: https://docs.suricata.io/en/suricata-6.0.0/rules/header-keywords.html?highlight=offset#ipv6-hdr
https://www.kali.org/tools/thc-ipv6/#atk6-kill_router6

Mitigación de vulnerabilidades

Configuración de reglas de filtrado en Nokia SRL Linux

La elección: Nokia Service Router Linux. Características.

- Standard Linux Kernel no modificado.
- Imagen Docker Container disponible sin requerimientos de licencia de uso.
- Startup time 1min aprox. Bajo consumo de recursos (2vCPU y 2Gb RAM).
- Arquitectura modular.
- Permite definir instancias de red, (Layer 2, Layer 3).
- Gran flexibilidad para la definición de ACLs

Fuentes: https://learn.srlinux.dev/

Mitigación de vulnerabilidades

Configuración de reglas de filtrado en Nokia SRL Linux

Configuraciones iniciales:

Image: srlinux 23.10.1
Network instance default
IPv6 link local static: fe80::1:2/64
IPv6 global unicast static: 2001:db8:aaaa:1::1
Router adviertisement prefix 2001:db8:aaaa:1::/64
startup-config: srlrt/config.json

Image: srlinux 23.10.1
Network instance lanswitch
Interfaces type bridged
ACL ipv6filter y logging
startup-config: srlsw/config.json

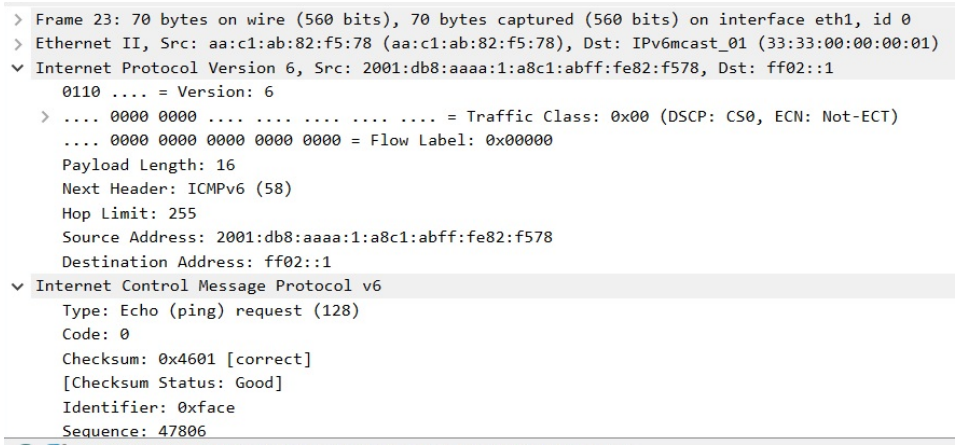
Se configuró logging local, visualización de logs: `show system logging file ipv6acl`

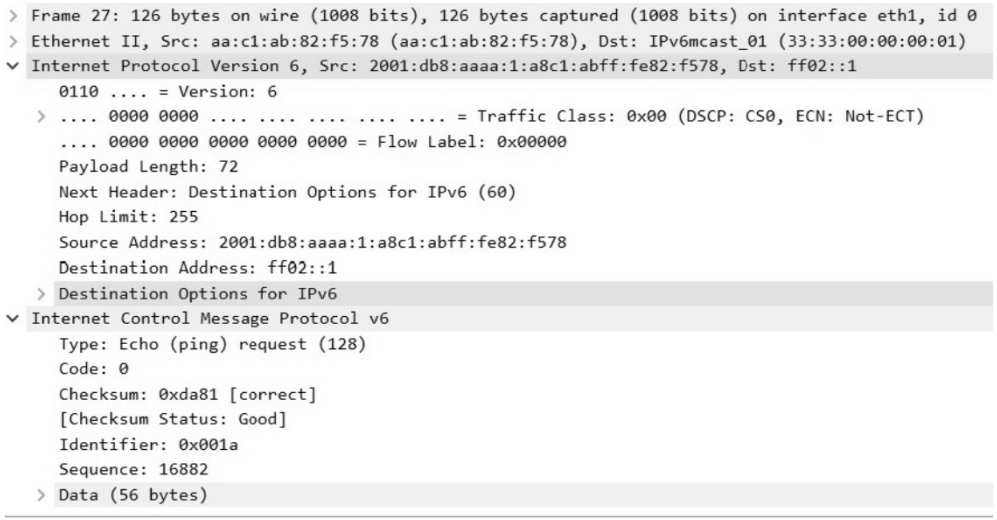
Fuentes: https://learn.srlinux.dev/
https://documentation.nokia.com/srlinux/23-10/index.html

Mitigación de vulnerabilidades

Configuración de reglas de filtrado en Nokia SRL Linux

Escenario 1: Mitigación de escaneo de red local: `scan6 -i eth1 -L`
En base a lo expuesto en RFC 7707 Sección 4.3, más captura y análisis de encabezados ICMPv6.





Fuentes: https://datatracker.ietf.org/doc/html/rfc7707

Mitigación de vulnerabilidades

Configuración de reglas de filtrado en Nokia SRL Linux

Escenario 1: Mitigación de escaneo de red local: `scan6 -i eth1 –L`
En base a lo expuesto en RFC 7707 Sección 4.3, más captura y análisis de encabezados ICMPv6. Se configura en nodo Nokia SRL Linux (srl1), una **acl ipv6 filter "ipv6ra" entrys…**

Encabezado IPv6	Origen	Destino
Next Header ICMPv6 (58)	IPv6 addr global unicast PC2	ff02::1
ICMPv6 Type 128		
Code 0		

Encabezado IPv6	Origen	Destino
Next Header Dest Opt for IPv6 (60)	IPv6 addr global unicast PC2	ff02::1
ICMPv6 Type 128		
Code 0		

```
entry 60 {
        action {
            drop {
                log true
            }
        }
        match {
            next-header 60
            destination-ip {
                prefix ff02::/127
            }
        }
```

```
entry 70 {
        action {
            drop {
                log true
            }
        }
        match {
            next-header icmp6
            destination-ip {
                prefix ff02::/127
            }
            icmp6 {
                type 128
                code [
                    0
                ]
            }
```

Mitigación de vulnerabilidades

Configuración de reglas de filtrado en Nokia SRL Linux

Escenario 2: Mitigación ataque fake router advertisement: `atk6-fake_router6 eth1 2001:db8:dddd:1::/64`

En base a lo expuesto en RFC 6105 Sección 3, más captura y análisis de encabezados ICMPv6.

Encabezado IPv6	Origen	Destino
ICMPv6 Type RA (134)	IPv6 addr link local PC2	ff02::1
Code 0		
ICMPv6 Option Prefix: 2001:db8:dddd:1::/64		
ICMPv6 Option Route info: High		

```
entry 100 {
        action {
            drop {
                log true
            }
        }
        match {
            next-header 58
            icmp6 {
                type 134
                code [
                    0
                ]
            }
```

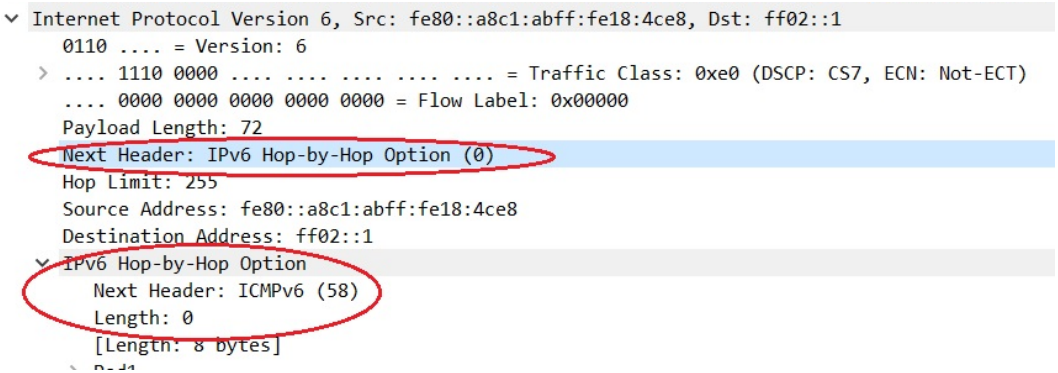
Fuentes: https://datatracker.ietf.org/doc/html/rfc6105
https://www.kali.org/tools/thc-ipv6/#atk6-fake_router6

Mitigación de vulnerabilidades

Configuración de reglas de filtrado en Nokia SRL Linux

Escenario 3: Mitigación fake RA vector de ataque basado en Extension Headers: `atk6-fake_router26 -E H111 -A 2001:db8:cccc:1::/64 eth1`

En base a lo expuesto en RFC 7113 Sección 2.1, más captura y análisis de encabezados ICMPv6.




```
entry 90 {
        action {
          drop {
            log true
          }
        }
        match {
          match {
            next-header ipv6-hop
            destination-ip {
              prefix ff02::/127
        }
      }
```

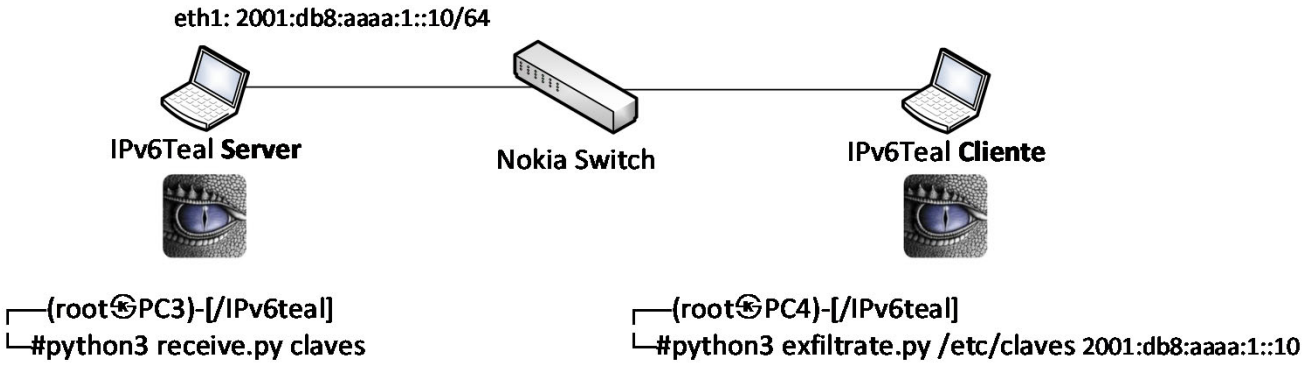
Fuentes: https://datatracker.ietf.org/doc/html/rfc7113
https://www.kali.org/tools/thc-ipv6/#atk6-fake_router26

Mitigación de vulnerabilidades

Exfiltración de datos vía el campo de encabezado IPv6 flowlabel.

Este campo se puede utilizar para crear canales de comunicación secretos, almacenando y transmitiendo datos sin que el tráfico se identifique como sospechoso.

Escenario 4: Exfiltración de datos con IPv6teal. El script de exfiltración envía 1 paquete IPv6 por cada 20 bits de datos y el script del receptor reconstruye los datos leyendo el campo flowlabel.

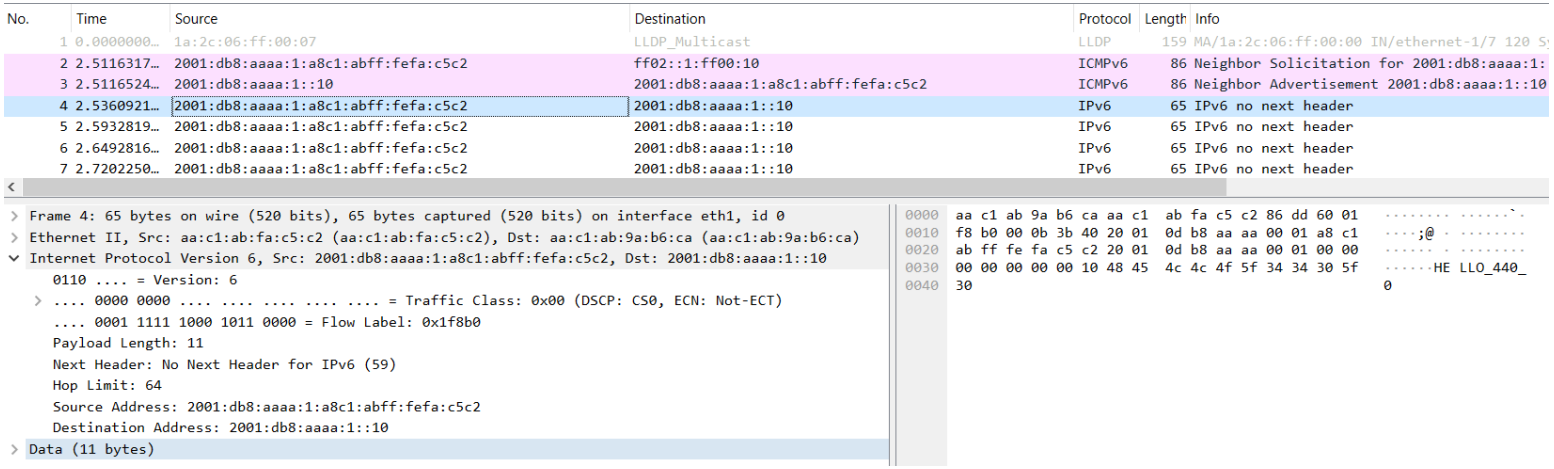


Fuentes: https://github.com/christophetd/IPv6teal
https://blog.lacnic.net/los-riesgos-de-ignorar-ipv6-en-su-red/

Mitigación de vulnerabilidades

Exfiltración de datos vía el campo de encabezado IPv6 flowlabel.

Escenario 4: Exfiltración de datos con IPv6teal. Análisis de captura de tráfico




```
entry 20 {
        action {
            drop {
                log true
            }
        }
        match {
            next-header 59
        }
    }
```

Fuentes: https://datatracker.ietf.org/doc/html/rfc6437#page-3

Consideraciones sobre las Cabeceras de Extensión

Estandarización IPv6 RFC 8200 (STD86). Jordi Palet

Procesadas solo por los nodos destino. A excepción de Hop by Hop Options Header

Para “regular” la creación de nuevas cabeceras de extensión se establecen algunas reglas y un formato, (RFC 6564).

Se debe preferir el uso de Destination Options para mandar información, en la cabecera Destination Options ya existente.

Se debe evitar la creación de cabeceras de extensión con comportamiento Hop by Hop y crear nuevas opciones para esa cabecera de extensión, siempre que sea posible .

Por Compatibilidad , no se deben crear nuevas cabeceras de extension a no ser que no se pueda usar ninguna opción nueva en las cabeceras ya existentes.

Consideraciones de seguridad: Generalidades

Monitorizar el tráfico de red. Que se considera tráfico normal? En el contexto de una LAN IPv6, la naturaleza de las aplicaciones requieren el uso de campos de extensión?. MTU común en todo el segmento.

Análisis exhaustivo de las técnicas de ataque requiere un “Deep packet inspection”. Definir umbrales de tráfico normal para ICMPv6 en la red.

Revisión de RFCs, políticas de seguridad y recomendaciones de buenas prácticas. Lecturas recomendadas: “IPv6 Node Requirements draft-clw-6man-rfc8504-bis-01” y “RFC 9099: Operational Security Considerations for IPv6 Networks”.

Trabajos a futuro

Análisis de seguridad en una topología configurada con DHCPv6 Stateless y Statefull.

Análisis de seguridad en alternativas de transición, Dual Stack, traducción de direcciones con SIIT Jool.

Deploy de nuevas topologías para test de seguridad a dispositivos firewall, switchs, routers de diferentes fabricantes.

Obrigado !
Muchas gracias !
Preguntas ???

Ernesto Sánchez
linkedin.com/in/ernestosánchez

Henri Alves de Godoy
linkedin.com/in/henri-alves-godoy

UNICAMP

UCASAL
UNIVERSIDAD CATÓLICA DE SALTA

educorp
Escola de **Educação** **Corporativa** da Unicamp

UNSa
Universidad
Nacional de Salta