



DETECCIÓN Y MITIGACIÓN DE ATAQUES DoS Y DDoS CON MIKROTIK

Ing. Francisco Méndez

MikroTik Certified Trainer ID **#TR0491**

Presentador

Ing. Francisco Méndez

- MikroTik Certified Trainer ID #TR0491
- Telecommunications Engineer.
- Master in Satellite Engineering.
- Oracle Java SE7 Certified Programmer.

Cursos y Certificaciones

Ing. Francisco Méndez - Trainer

 fm@mkx.cl



 academy xperts

Asesoría y Soporte

Ing. Francisco Méndez - Gerente de Proyectos



fm@eruditum.cl

- Soluciones BGP
- Balanceo de Carga
- Firewall Avanzado
- Anti-DDoS
- Calidad de Servicio (QoS)
- VPN
- Hotspot
- Soluciones inalámbricas
- Soporte mensual
 - ✓ Mantenimiento preventivo
 - ✓ Monitoreo
 - ✓ NOC 24/7



Eruditum
We Know!

Enlaces Dedicados

Ing. Francisco Méndez - Gerente de TI

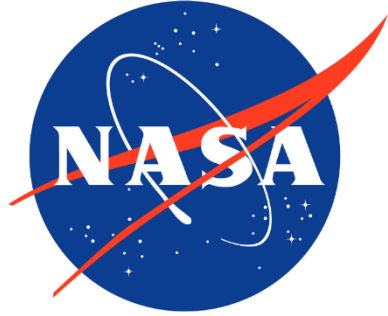


fm@austrointernet.cl

- Conexión con CDN (Content Delivery Network)
- Reducción de consumo de ancho de banda internacional
- Protección **Anti-DDoS** incluida
- Mejores **costos** del mercado



Algunos clientes felices



Ataques

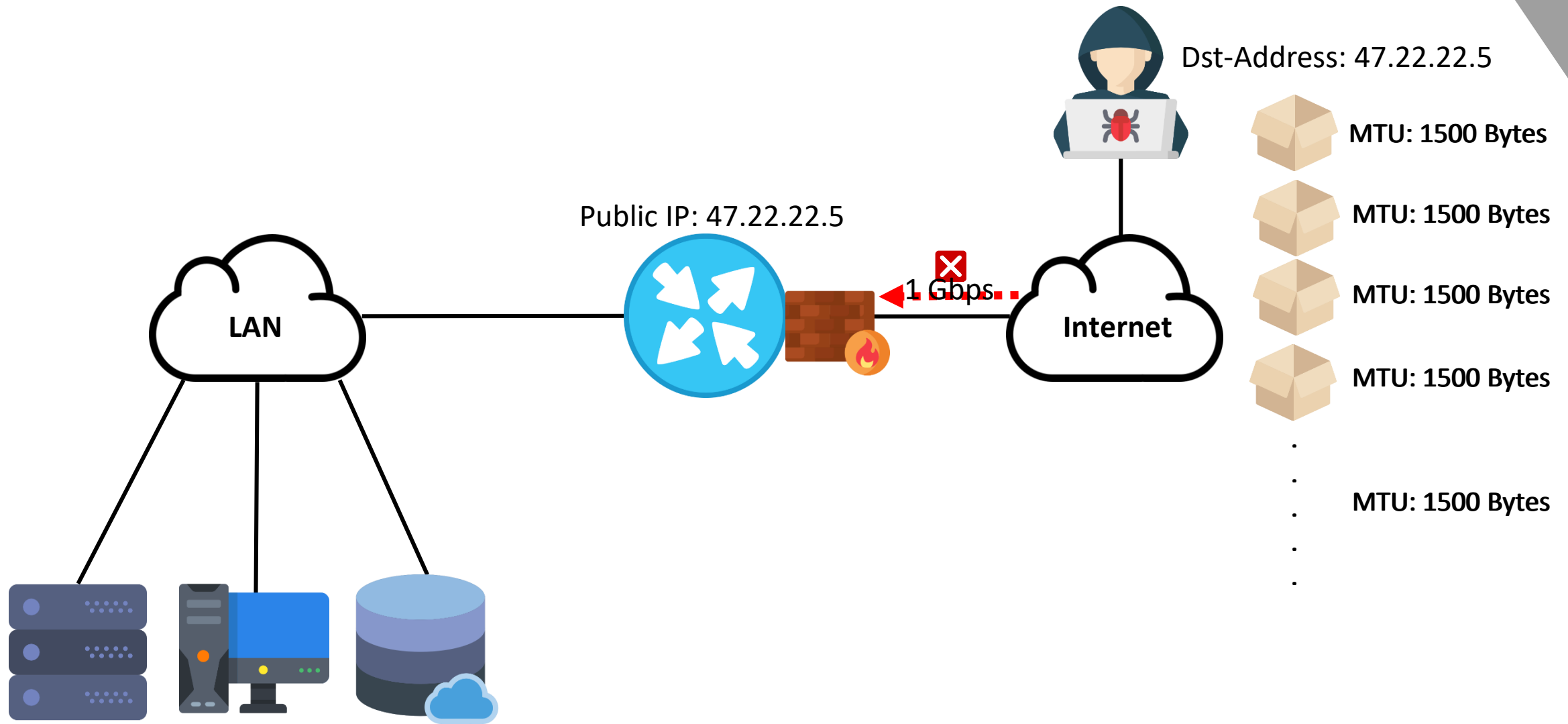
DoS: Denial of Service.

DDoS: Distributed Denial of Service



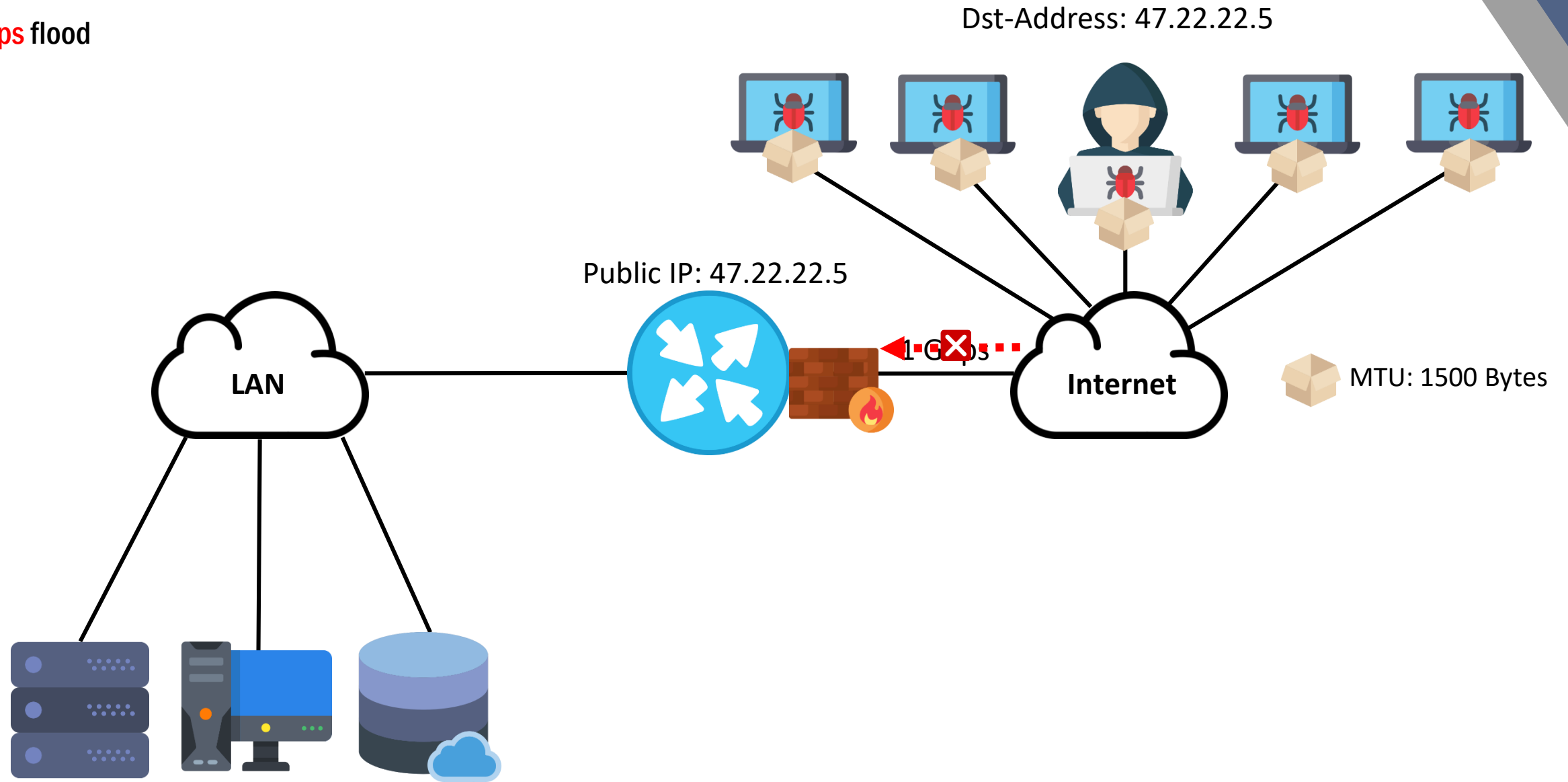
DoS: Denial of Service

Mbps flood



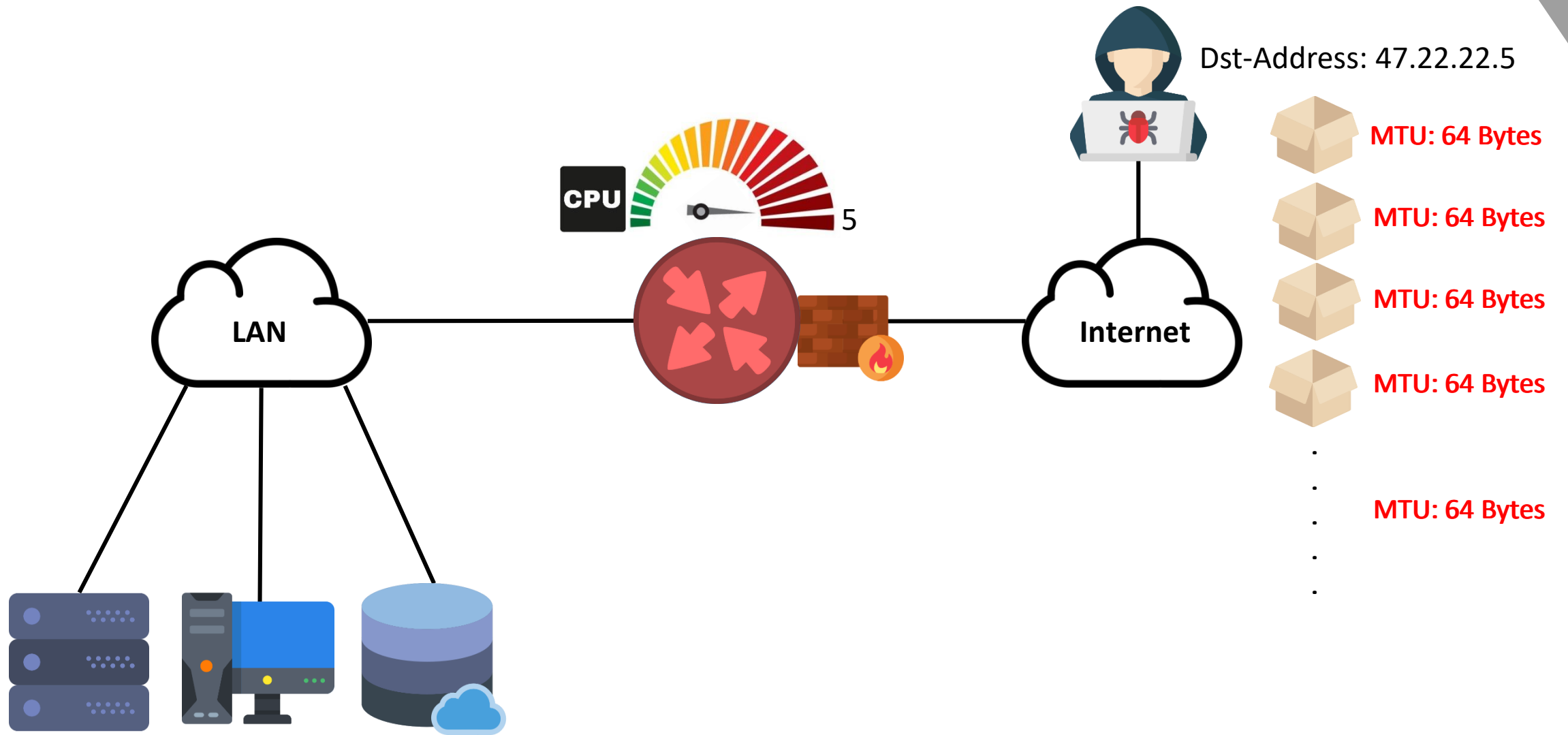
DDoS: Distributed Denial of Service

Mbps flood



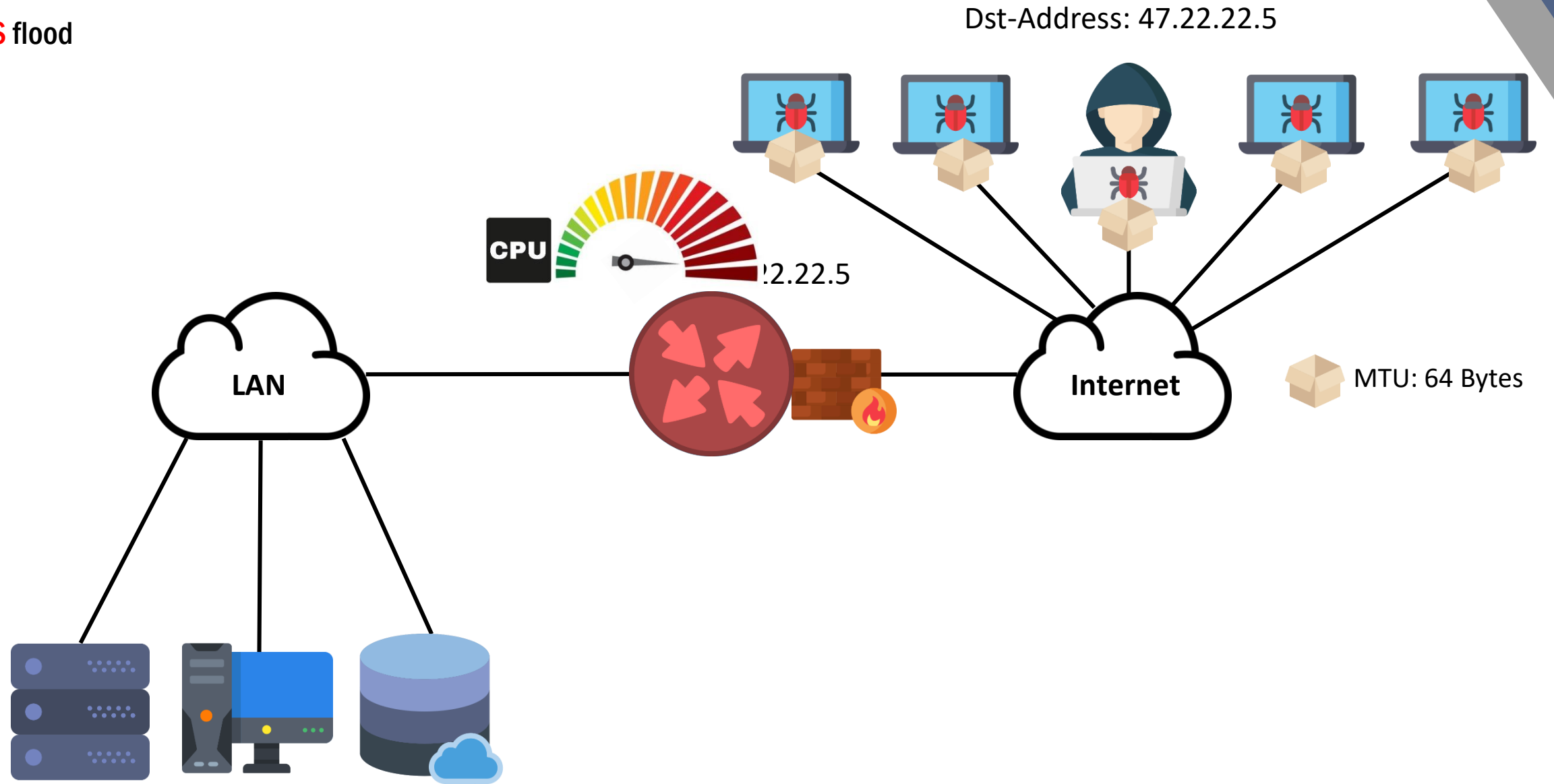
DoS: Denial of Service

PPS flood



DDoS: Distributed Denial of Service

PPS flood



Protocolo de ataque

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)



Posibles soluciones

1. Ancho de banda suficiente + buen Firewall.
2. Solicitar Blackhole al ISP.
3. Peer BGP con servicios de mitigación.

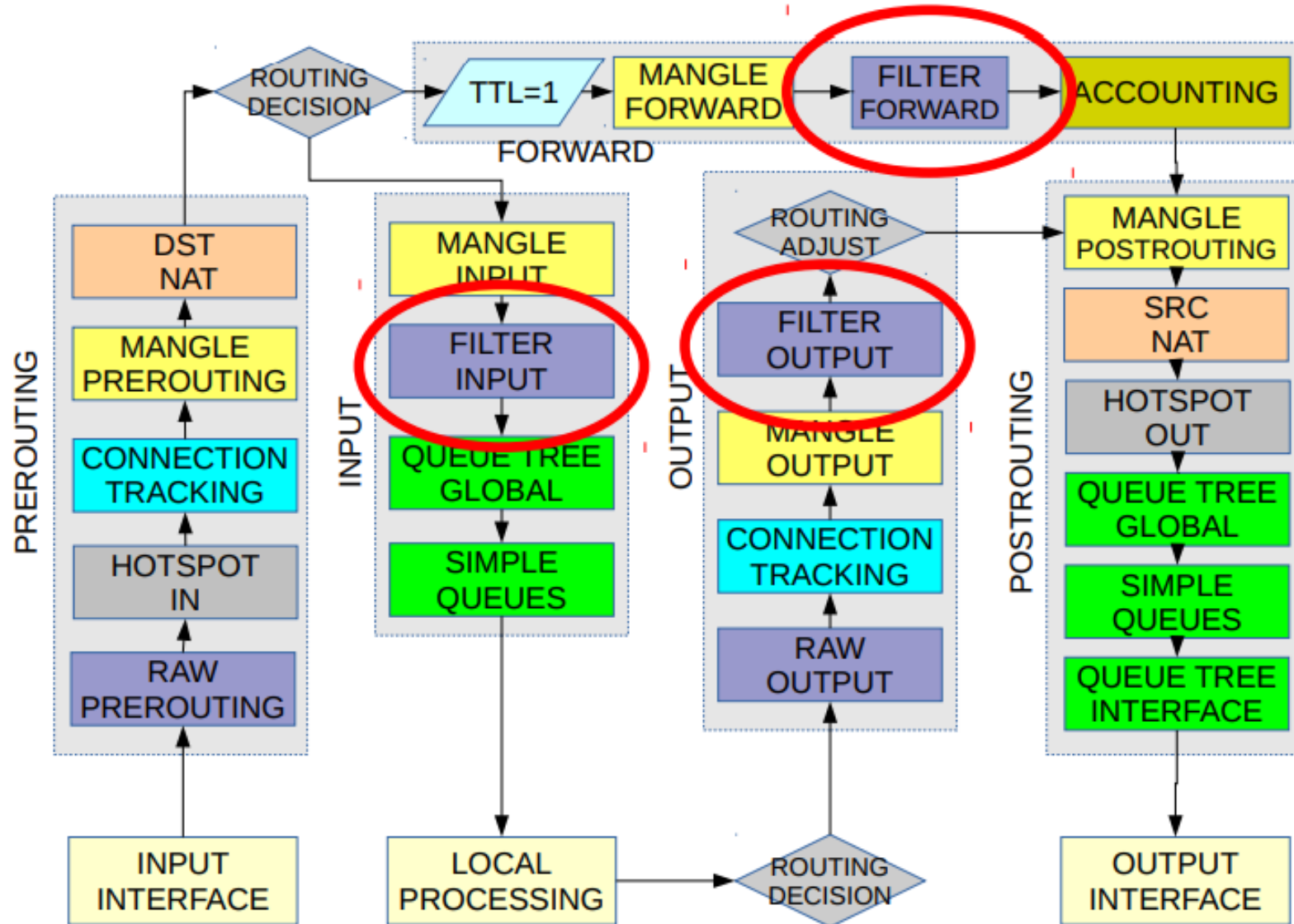
Posibles soluciones

1. Ancho de banda suficiente + buen Firewall.

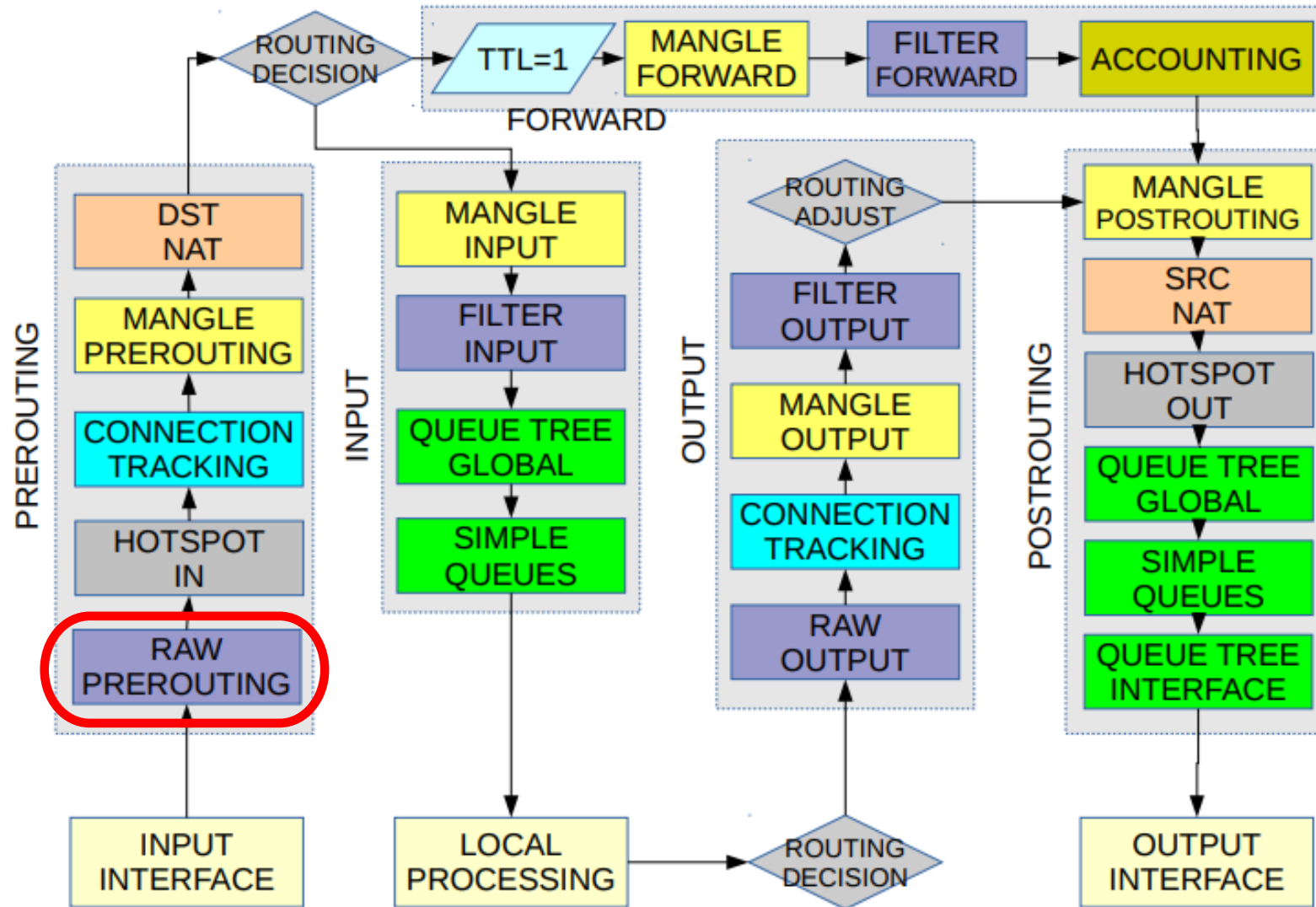
- Se recomiendan enlaces con capacidades superiores a 1Gbps.
- Buen Hardware dedicado a Firewall, **CCR1036** o **CCR1072**
- Para ataques **TCP, Tarpit** y limite de **SYN**.
- Para ataques **UDP, drop** del puerto en **Firewall RAW**.
- Evitar reglas de Log.



Esquema Firewall Filter



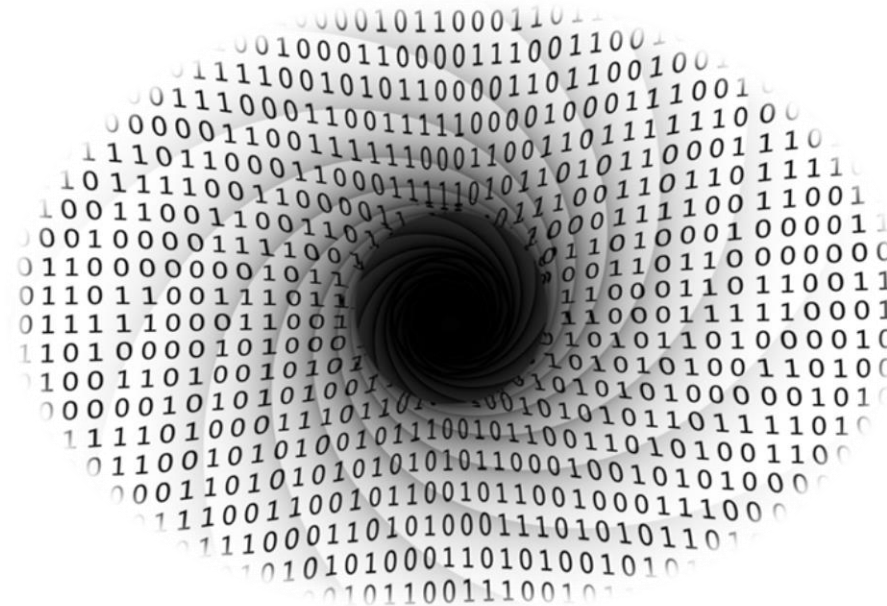
Esquema Firewall Raw



Posibles soluciones

2. Solicitar Blackhole al ISP.

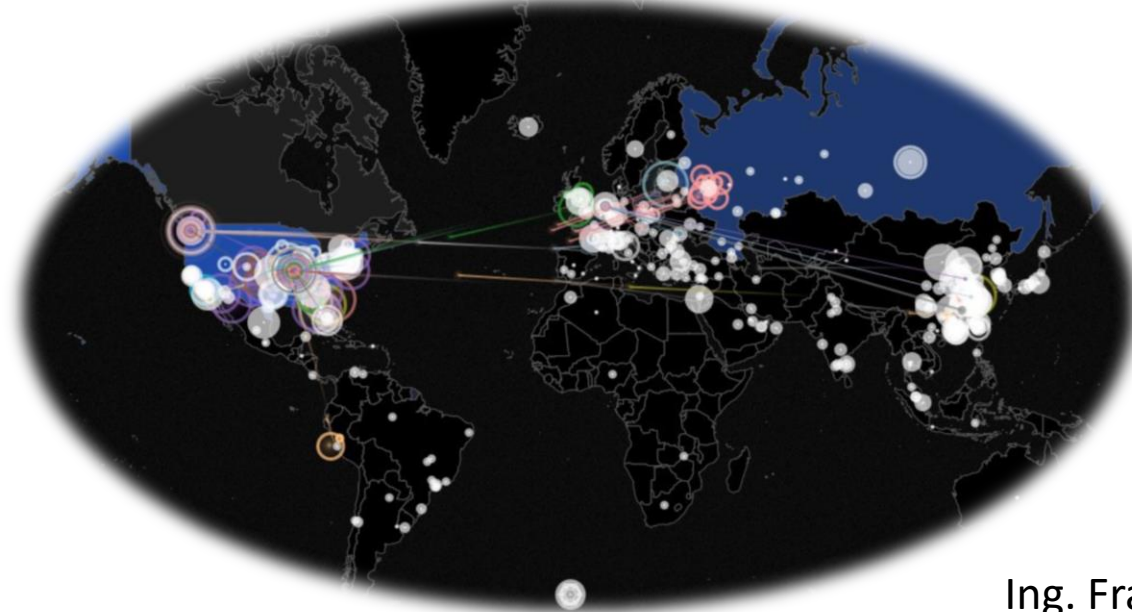
- Se debe tener acordado un **servicio de Blackhole** con el ISP.
- La manera mas **eficiente** es a través de **BGP Community**.
- Sin BGP Community depende del **tiempo de respuesta** del ISP.
- La **IP/32** enviada a Blackhole **no puede ser utilizada**.



Posibles soluciones

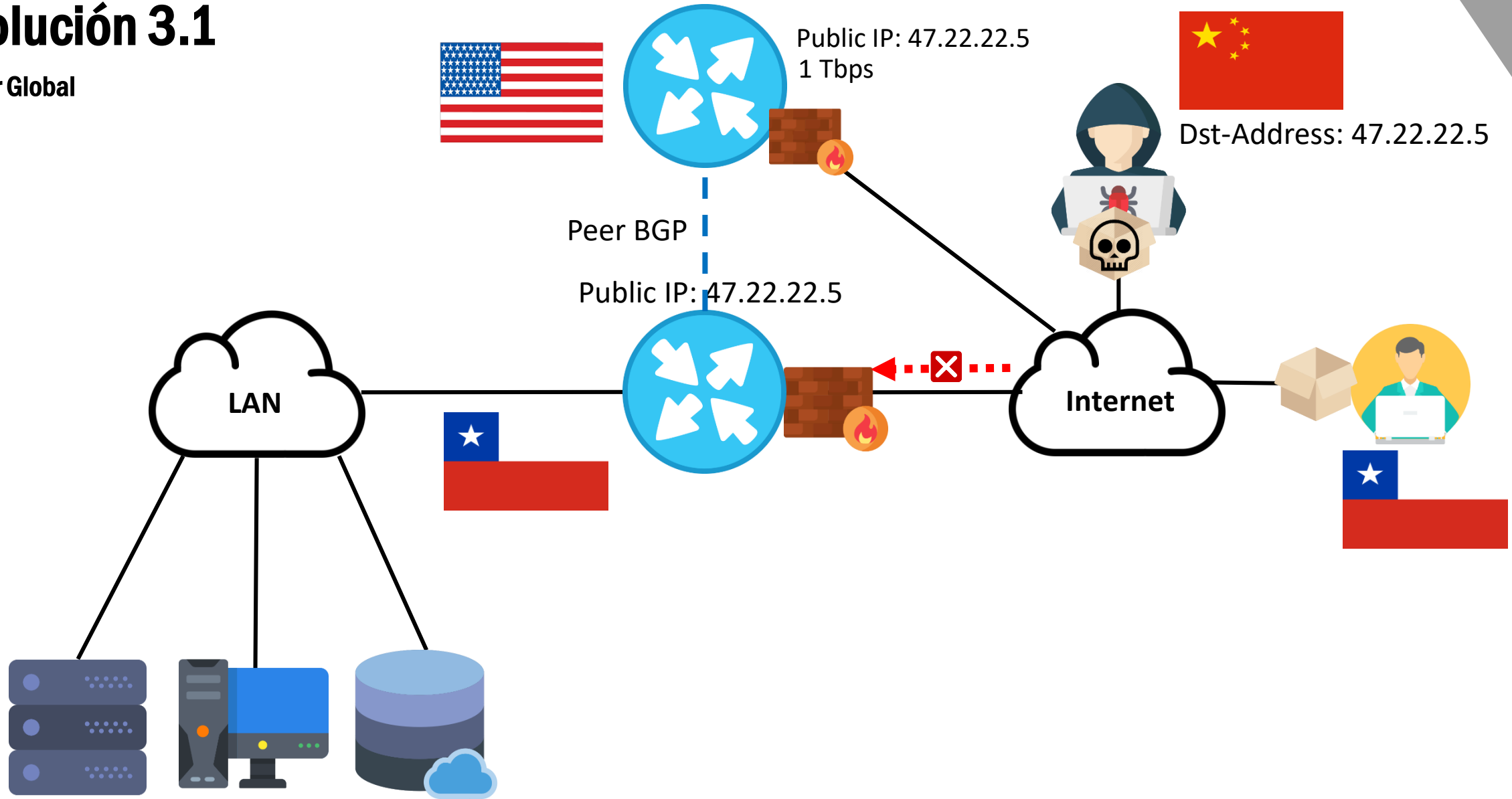
3. Peer BGP con servicios de mitigación.

- Se debe **tener** un **ASN** con prefijos mínimo /24
- Peer BGP con algún **proveedor especializado** en mitigación idealmente fuera del país
- La solución puede ser más potente si se tiene **separación** de peers BGP por tráfico **Nacional e Internacional**



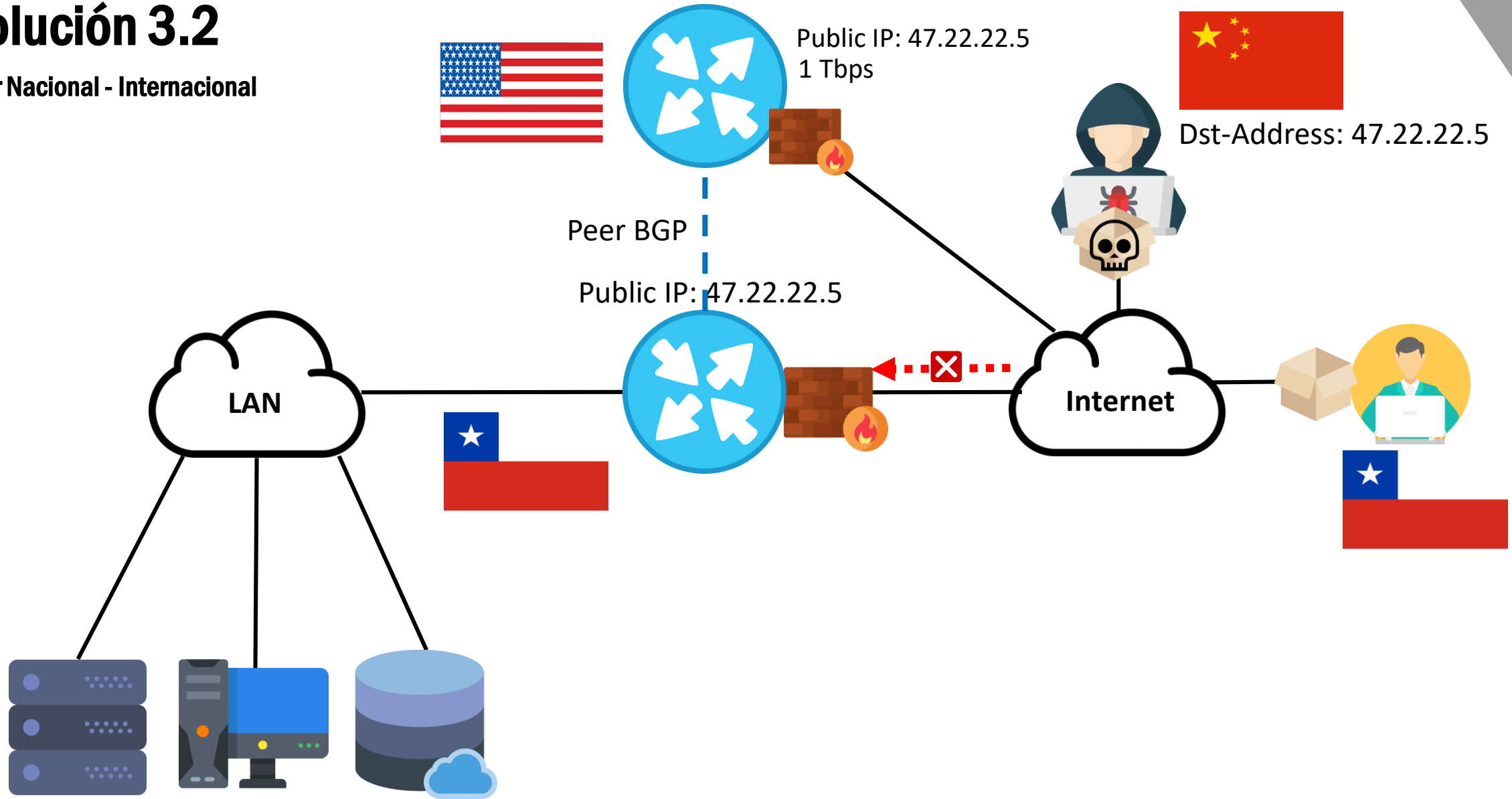
Solución 3.1

Peer Global



Solución 3.2

Peer Nacional - Internacional



Estadísticas Firewall Raw

Firewall											
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols											
+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters											
#	Action	Chain	! Dst. Address	! : : : : (In. Interface List	Src. Address List	! Jump Target	Bytes	Packets	Comment	
81	jump	prerouting			internet		mirror	15407.6 GiB	36718 818 301	stats	
82	passthrough	mirror				nacional		12763.1 GiB	29446 122 955	stats	
83	passthrough	mirror				!nacional		2644.6 GiB	7272 695 342	stats	
84	return	mirror	0/24			nacional		2893.7 GiB	3233 283 076	stats	
85	return	mirror	0/24			nacional		977.7 GiB	2827 113 125	stats	
86	return	mirror	0/24			nacional		34.9 MiB	824 372	stats	
87	return	mirror	0/24			nacional		498.5 GiB	2193 385 108	stats	
88	return	mirror	0/24			nacional		1540.7 GiB	6345 435 148	stats	
89	return	mirror	0/24			nacional		39.5 MiB	874 287	stats	
90	return	mirror	0/24			nacional		17.5 GiB	113 321 216	stats	
91	return	mirror	0/24			nacional		10.9 GiB	10 115 597	stats	
92	return	mirror	!0/24			nacional		196.7 GiB	787 008 161	stats	
93	return	mirror	!0/24			nacional		1082.5 GiB	5140 655 272	stats	
94	return	mirror	!0/24			nacional		4440.5 GiB	5850 900 538	stats	
95	return	mirror	!0/24			nacional		1104.2 GiB	2943 207 055	stats	
96	return	mirror	0/22			nacional		0 B	0	stats	
97	return	mirror	0/23			nacional		0 B	0	stats	
98	return	mirror	45.238.179.0/24			nacional		0 B	0	stats	
99	return	mirror	!0/24			!nacional		111.6 GiB	656 589 247	stats	
100	return	mirror	!0/24			!nacional		128.7 GiB	506 888 985	stats	
101	return	mirror	!0/24			!nacional		1151.8 MiB	17 616 180	stats	
102	return	mirror	!0/24			!nacional		303.4 GiB	1456 098 262	stats	
103	return	mirror	!0/24			!nacional		256.1 GiB	1076 138 878	stats	
104	return	mirror	!0/24			!nacional		909.5 MiB	15 301 357	stats	
105	return	mirror	!0/24			!nacional		61.9 GiB	103 389 203	stats	
106	return	mirror	!0/24			!nacional		7.0 GiB	20 280 768	stats	
107	return	mirror	!0.0/24			!nacional		87.4 GiB	395 204 839	stats	
108	return	mirror	!1.0/24			!nacional		212.4 GiB	718 339 464	stats	
109	return	mirror	!2.0/24			!nacional		1293.9 GiB	1675 120 787	stats	
110	return	mirror	!3.0/24			!nacional		180.2 GiB	631 727 664	stats	
111	return	mirror	!0/22			!nacional		0 B	0	stats	
112	return	mirror	!0/23			!nacional		0 B	0	stats	
113	return	mirror	45.238.179.0/24			!nacional		0 B	0	stats	

Estadísticas Firewall Raw

```
[eruditum@1036-PRODv2] > ip firewall raw print stats where dst-address="45.238.179.0/24" and src-address-list="!nacional"
Flags: X - disabled, I - invalid, D - dynamic
# CHAIN ACTION BYTES PACKETS
0 ;;; stats mirror return 1 389 516 95... 1 675 353 593
[eruditum@1036-PRODv2] > ip firewall raw print stats where dst-address="45.238.179.0/24" and src-address-list="nacional"
Flags: X - disabled, I - invalid, D - dynamic
# CHAIN ACTION BYTES PACKETS
0 ;;; stats mirror return 4 768 261 16... 5 851 364 382
```

```
bytes_diff = Val(mk_bytes) - Val(sql_bytes)
Console.WriteLine("bytes_diff = " + bytes_diff.ToString("N0"))

mbps = Val(bytes_diff) / segundos_diff
mbps = mbps * 8 / (1024 * 1024)
mbps_str = mbps.ToString("F0")













pps = Math.Abs(Val(sql_packets) - Val(mk_packets)) / segundos_diff
pps_str = pps.ToString("F0")
```

Peers BGP

BGP

Instances VRFs Peers Networks Aggregates VPN4 Routes Advertisements

+ - ✓ ✗ [Message Icon] [Filter Icon] Refresh Refresh All Resend Resend All

Name	Instance	Uptime	Prefix Co...	State
 austro	default	17d 21:55:19	11	established
 facebook	default	15d 07:09:51	34	established
 google	default	15d 07:09:53	579	established
 ifx	default	14d 12:53:59	5509	established
 level3_internacional	default	54d 06:02:48	1	established
 level3_nacional	default	54d 06:02:48	5717	established
 microsoft 1	default	15d 07:09:52	212	established
 microsoft 2	default	15d 07:09:52	212	established
 pitchile-1	default	15d 07:22:17	5170	established
 pitchile-2	default	15d 07:21:33	5265	established
 stomwall-ifx	default	2d 18:06:16		established
 stomwall-level	default	2d 18:04:25		established

Filtros BGP


Route Filters


+ - ✓ ✗ 📁 🏠

Prefix in 45.238.179.0/24

#	Chain	Prefix		Action	Comment
36	stomwall-out	45.238.179.0/24	:	accept	45.238.179.0/24-STR
37	stomwall-out	45.238.179.0/24		accept	45.238.179.0/24-STR
55	nacional-out	45.238.179.0/24		accept	45.238.179.0/24-ISP
72	intemacional-out	45.238.179.0/24		accept	45.238.179.0/24-ISP
90	austro-in	45.238.179.0/24		accept	
110	ifx-out	45.238.179.0/24		accept	45.238.179.0/24-ISP
130	level3-out	45.238.179.0/24		accept	45.238.179.0/24-ISP
150	gtd-out	45.238.179.0/24		accept	45.238.179.0/24-ISP
170	sparkle-out	45.238.179.0/24		accept	45.238.179.0/24-ISP

Sistema de Detección y Mitigación

Francisco



- Monitor
- VLANs
- Parámetros

Parámetros

Umbrales Ataques

Duración de Alerta (min)

Límite Internacional Mbps

Límite Internacional Pps

Sensibilidad Internacional (x 5seg)

Límite Nacional Mbps

Límite Nacional Pps

Sensibilidad Nacional (x 5seg)

Umbrales Incidencias

Duración de Alerta (min)

Límite Internacional Mbps

Límite Internacional Pps

Sensibilidad Internacional (x 5seg)

Límite Nacional Mbps

Límite Nacional Pps

Sensibilidad Nacional (x 5seg)

Umbrales Router

Límite Input Mbps

Límite Input Pps

Límite % CPU

Límite % RAM

Generales

Período de muestreo (seg)

Antigüedad de datos (min)

Contacto

Correo

Celular

Sistema de Detección y Mitigación

The screenshot displays the Eruditum StormWall management interface. The top header includes the Eruditum logo with the tagline "We Know!" and the user name "Francisco". The left sidebar contains navigation options: "Monitor", "VLANs", and "Parámetros". The main content area features the "internetustro" logo and a grid of network interface monitors. Each monitor shows a status bar with a red dot indicating an alert and a red plus sign for expansion. The bottom-most monitor is highlighted with a tooltip showing the following statistics:

Interface	Alert
.0/22	Yes
.0/24	Yes
.0/24	Yes
.0/24	Yes
.0/24	Yes
.0/24	Yes
.0/24	Yes
.0/24	Yes
.0/24	Yes
.0/23	Yes
45.238.179.0/24	Yes

Highlighted Monitor Data:

- PPS: 41.473
- MBPS: 15
- BYTES: 46

Sistema de Detección y Mitigación

Eruditum
We Know!

Francisco ▾

Internet@USTRO

Monitor
VLANs
Parámetros

Monitor de Tráfico

CPU 3% RAM 15%

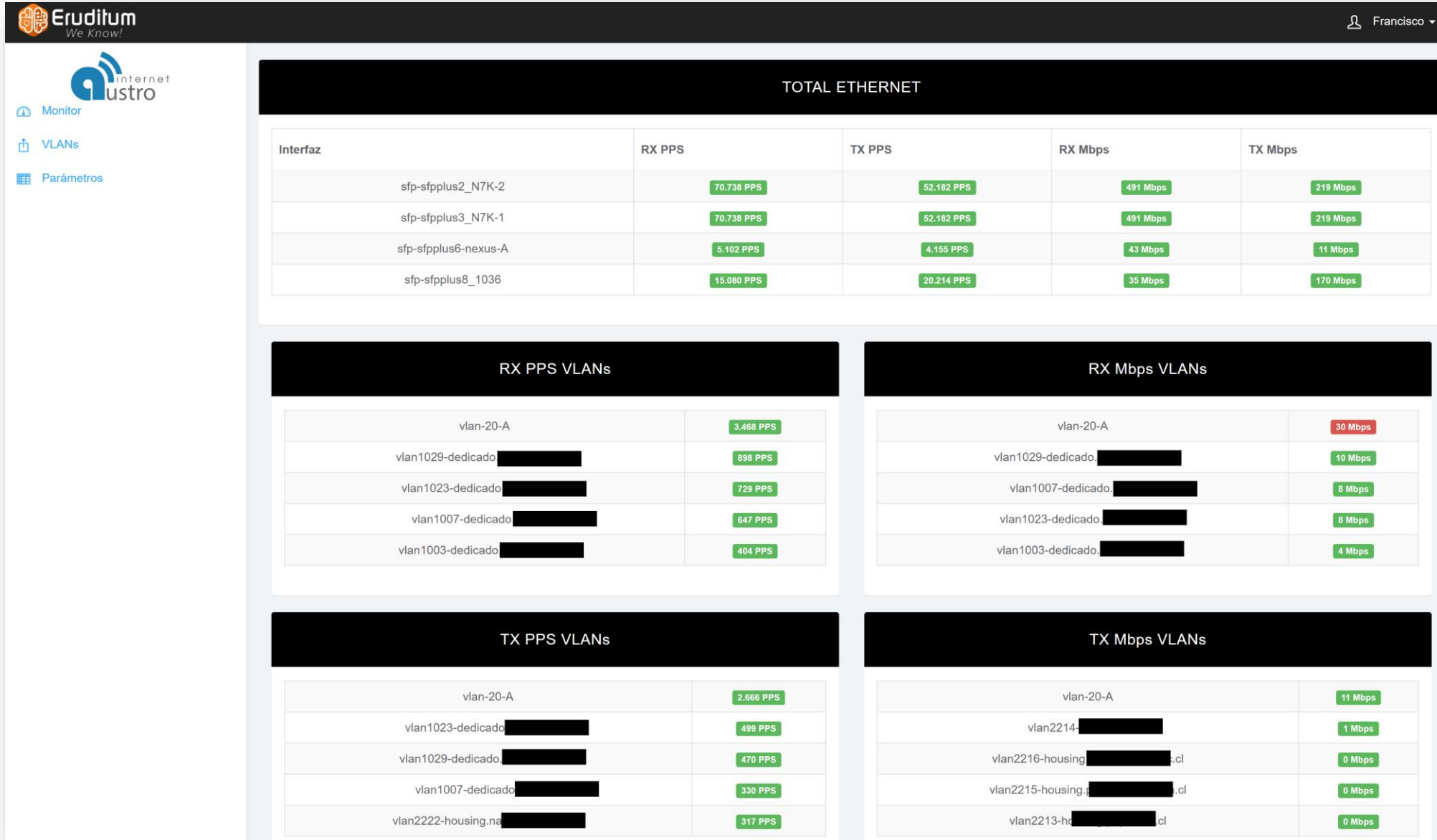
Internet@USTRO

		.0/22	
		.0/24	
		.0/24	
		.0/24	
		.0/24	
		.0/24	
		.0/24	
		.0/24	

StormWall™

		45.238.179.0/24	
--	--	-----------------	--

Sistema de Detección y Mitigación



Muchas Gracias!

