SOLUCIÓN ALTERNATIVA “LOW COST” PARA CONTROL DE ATAQUES VOLUMÉTRICOS EN LATINOAMÉRICA – Versión ISP

Arquitectura, funcionamiento y resultados

José Nilson Camargo Castro
jcamargo@ifxcorp.com
CO-IFNE-LACNIC

lacnic 33 online meeting

ifx Networks 20 AÑOS

ATAQUES VOLUMÉTRICOS LATAM

LA TEORÍA ES FUNDAMENTAL PERO….

ES MEJOR VERLA APLICADA EN EL MUNDO REAL

ATAQUES VOLUMÉTRICOS – Consideraciones Latam

- Soluciones de **Scrubbing Center** afectan latencias en Latam
- Soluciones de Scrubbing costosas y por dimensionamiento de BW
- Aprovechar los recursos de NAPs, CDNs, IxP
- Mayor responsabilidad en ISP Tier I y Tier II
- Objetivos potenciales ISP nivel tres o cuatro (WISP)
- Aún se presentan ataques debido a vulnerabilidades tipo memcached – Puerto 11211. **Amplificación muy grande.**
- **Se deben "explotar" los recursos disponibles que tiene BGP**

ANÁLISIS DE LOS ATAQUES VOLUMÉTRICOS

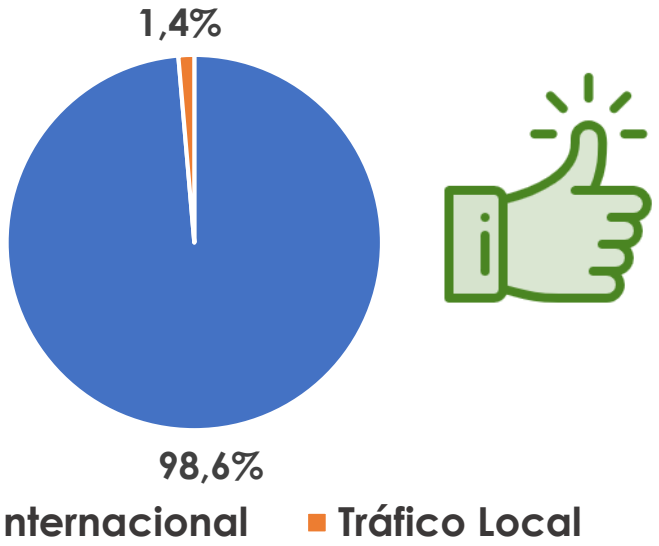
Tipos de ataques más comunes

- Inundación de tráfico UDP (Volumétricos)
- Ataques con tráfico TCP (No tan volumétricos pero si DoS)
- Puertos más conocidos
- Mayor tráfico internacional que nacional – BR(?)
- Fuerte presencia de países como USA, Rusia y países asiáticos.

Puertos usados más comunes

123 (NTP), 161 (SNMP), 53 (DNS)
0 – Paquetes modificados

Composición de los ataques

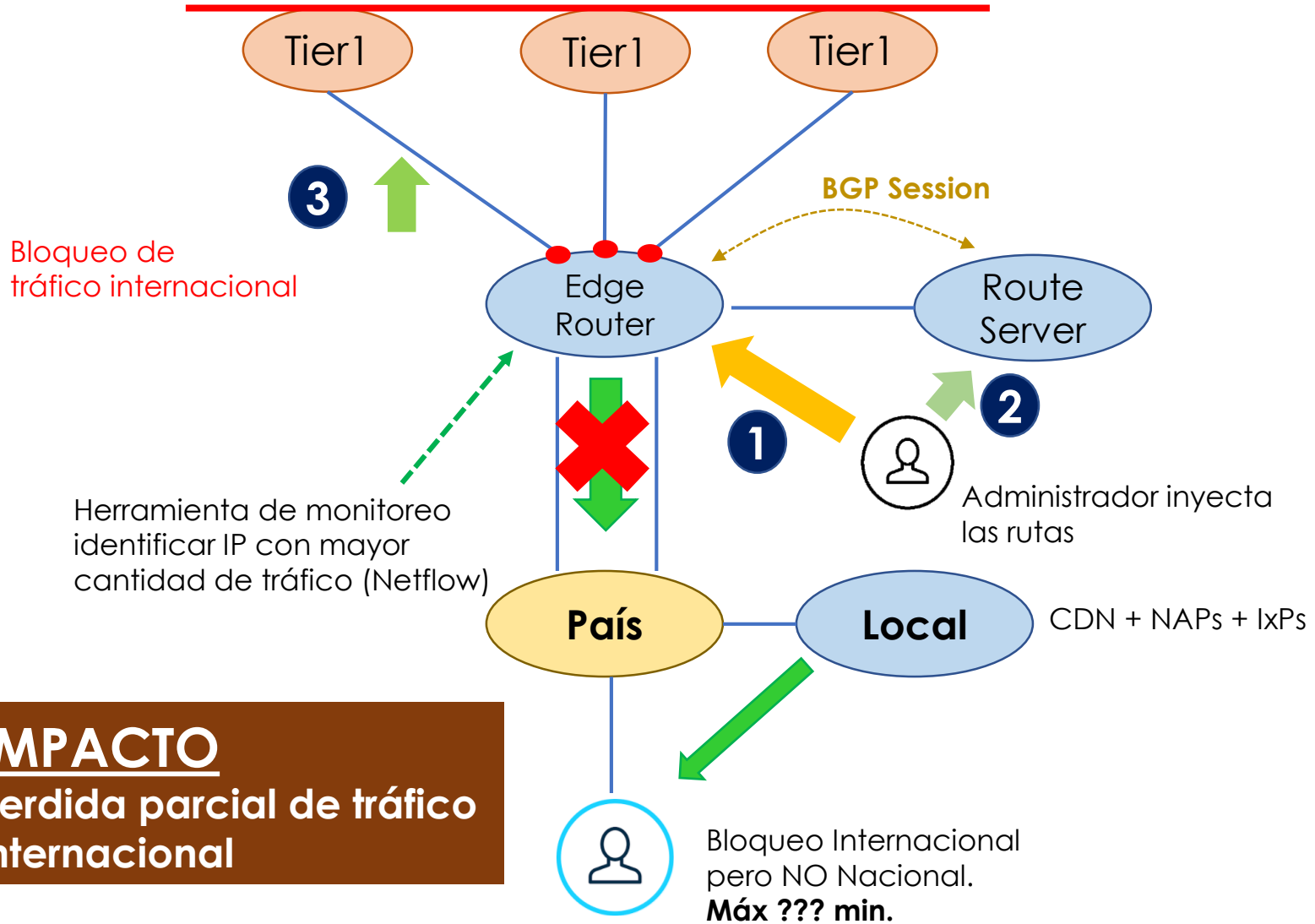


ARQUITECTURA PREVIA A LA IMPLEMENTACIÓN

1 RTBH Manual
Static Route + edge

2 RTBH Local
Router Server BGP + edge

RTBH Internacional
Router Server BGP +
3 Export RTBH Communities Tier I ISP



IMPACTO
Perdida parcial de tráfico internacional

DATOS PREVIOS A LA IMPLEMENTACIÓN

Identificación y resolución
Mayor a 2 horas

Ataques por mes
~ 45 ataques volumétricos > 1Gb

Impacto económico
Decenas de miles de USD

Ataques detectados
+ 10 ataques volumétricos > 10Gb

Ataques detectados
+ 5 ataques volumétricos > 20Gb

Impacto técnico
Inundación de puertas IP, degradación de servicios, saturación de troncales, perdida de servicio, etc…

VAMOS A VER CÓMO SE MEJORÓ ESTA SITUACIÓN…

ARQUITECTURA PROPUESTA

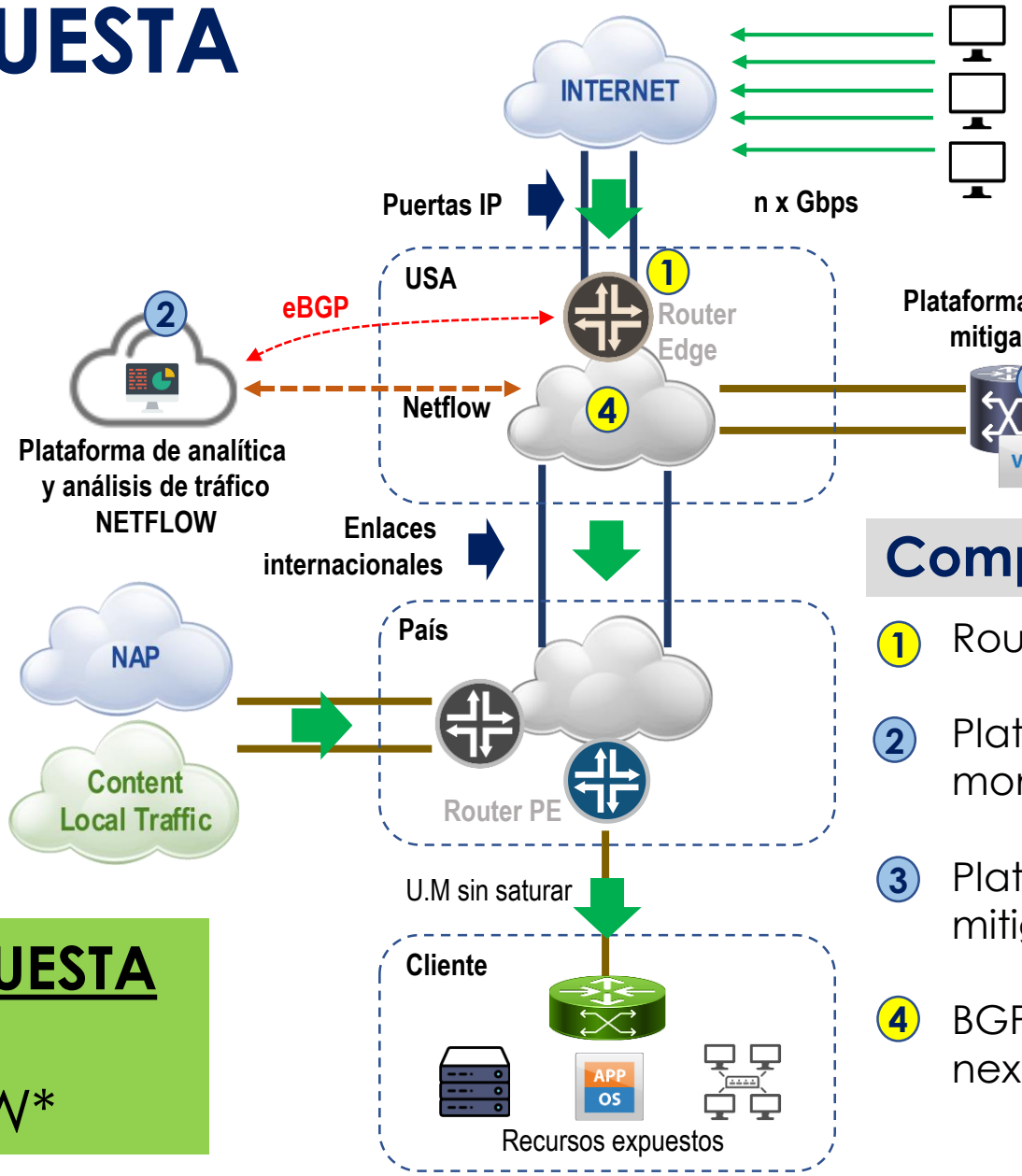
COSTO SOLUCIÓN FABRICANTE

- + USD 80.000 y adicionar Soporte Anual
- Soluciones por BW
- **Scrubbing Center(?) Latencia**

Son excelentes soluciones, pero un *entry level* requiere una alta inversión

COSTO ANUAL DE LA PROPUESTA

Menos de USD 8.000
Solución ilimitada en BW*

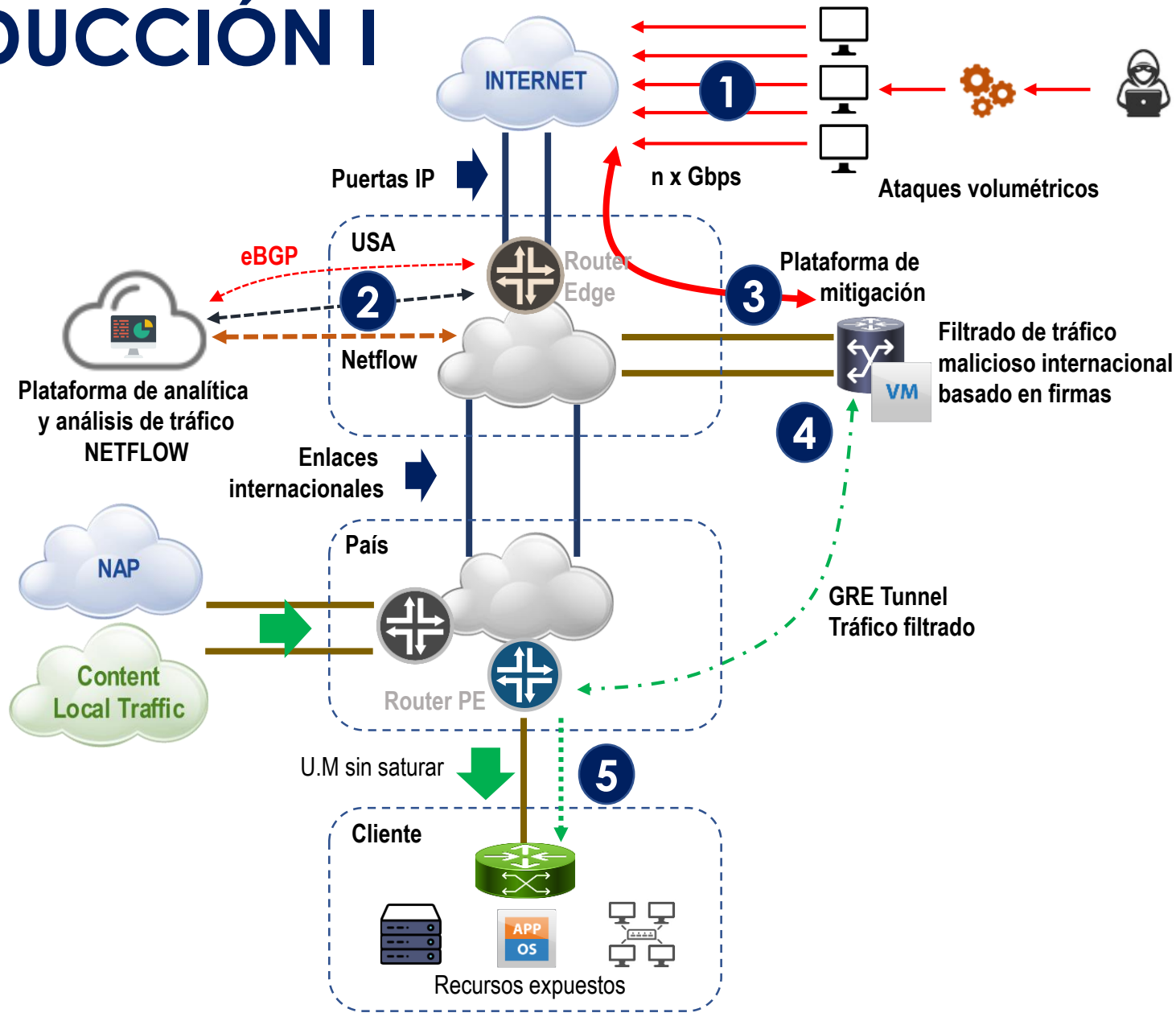


Componentes

1. Router Edge
2. Plataforma de monitoreo
3. Plataforma de mitigación. **"Free"**
4. BGP, Comunidades & next-hops, Tun. GRE

ESCENARIO EN PRODUCCIÓN I

1. Ingresa el tráfico malicioso a la red
2. La plataforma detecta el evento e inyecta la ruta BGP al Router Edge
3. El tráfico internacional se desvía al equipo de mitigación
4. Se aplica el filtro basado en firmas (L3 y L4) al tráfico y se envía por el *Clean Pipe*
5. El usuario final sigue recibiendo su tráfico nacional e internacional sin saturar su servicio en U.M

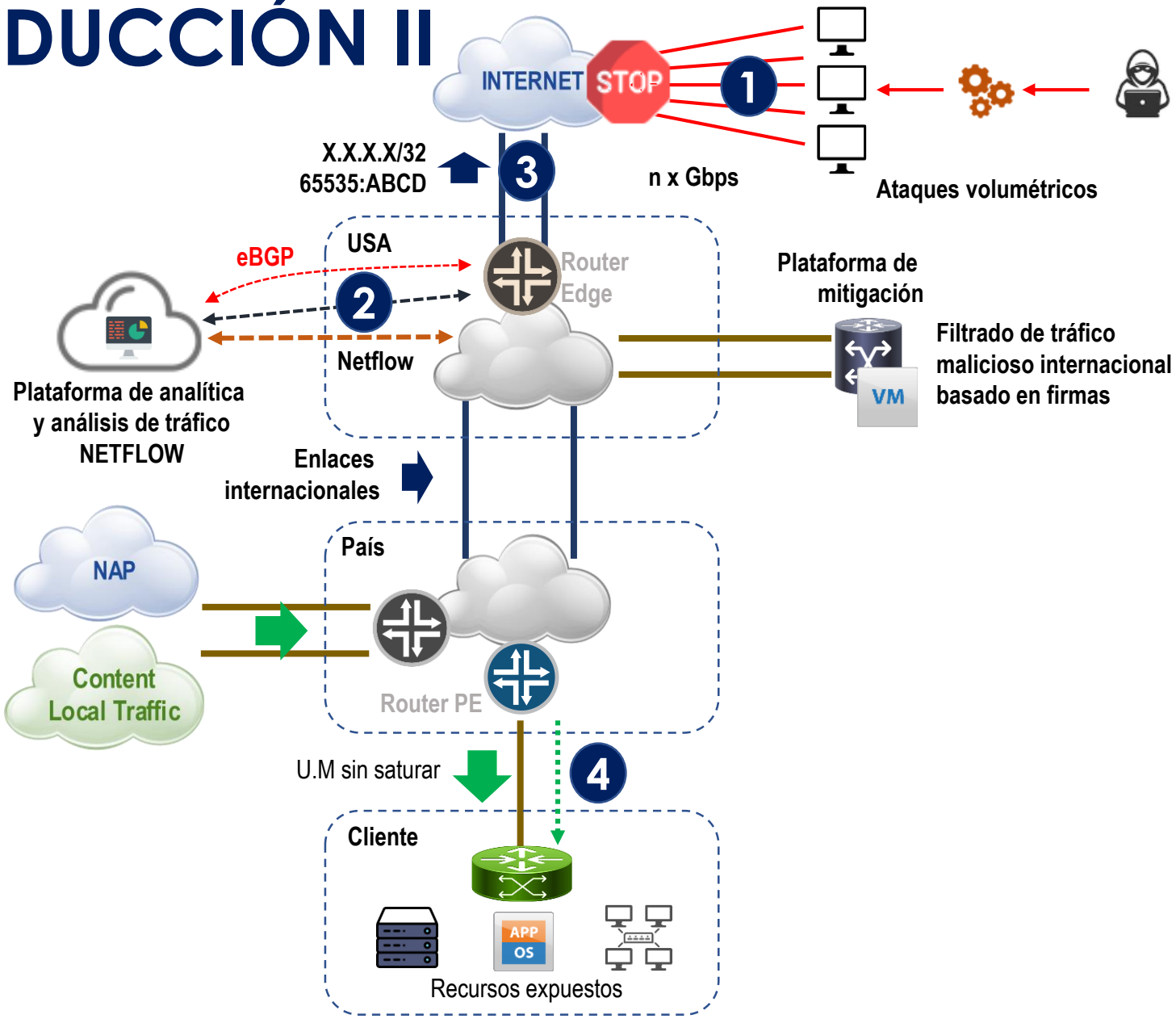


ESCENARIO EN PRODUCCIÓN II

¿Y si el ataque es muy grande y no se puede "limpiar"?

ISP Tier I – BGP communities

1. Ingresa el tráfico malicioso a la red
2. La plataforma detecta el evento e inyecta la ruta BGP al Router Edge
3. Se anuncia la ruta /32 a los *Tier I* con las *RTBH Communities* y se bloquea en los edge de ellos
4. El tráfico local-nacional nunca se afecta



RESULTADOS POSTERIORES A LA IMPLEMENTACIÓN

Identificación y resolución
Menor a 5 minutos

Operación automatizada
No intervención humana, excepto el análisis

Magnitud de ataques
Control sobre ataques de cualquier tamaño

Impacto económico
Minimizado – Casi cero

Impacto al cliente
Mínimo

Aumento de disponibilidad de la red

EJEMPLO REAL

El tiempo de "cuarentena" de la ruta se parametriza. Si el evento persiste, vuelve y se activa la ruta BGP.

CONCLUSIONES

- Aprovechar los recursos BGP como los RTBH Communities
- Invitación a los ISP a proporcionar este tipo de recursos de BGP
- Hay diferentes alternativas tanto en software como en hardware para desplegar soluciones de protección de ataques volumétricos, esto de acuerdo al poder adquisitivo de cada compañía.
- Explorar soluciones de este tipo que son parametrizables de acuerdo a los objetivos de la compañía

¡MUCHAS GRACIAS!

José Nilson Camargo Castro
jcamargo@ifxcorp.com
CO-IFNE-LACNIC

¿DUDAS O PREGUNTAS?

José Nilson Camargo Castro
jcamargo@ifxcorp.com
CO-IFNE-LACNIC