UNIVERSIDAD NACIONAL DE LA PLATA

ScrubUNLP: Mitigación de ataques de DDoS volumétricos

UNLP
Universidad **N**acional de **L**a **P**lata

Nicolás Macia / Alejandro Sabolansky
Mateo Durante / Cristian Daniel Barbaro

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Sobre CERTUNLP

UNIVERSIDAD NACIONAL DE LA PLATA

Misión de CERTUNLP:

- Gestionar incidentes de seguridad. Prevenir, detectar e investigar problemas de seguridad. Coordinar acciones para la protección de los usuarios y los servicios académicos de la UNLP.

Comunidad objetivo:

- Red de la UNLP:
  - Sistema Autónomo: 5692
  - Bloque IPv4: 163.10.0.0/16
  - Bloque IPv6: 2800:340::/32
- Dominio: *.unlp.edu.ar

Servicios:

- Gestión de Incidentes: análisis, Análisis Forense, Soporte en la solución, Coordinación
- Auditorías de seguridad de redes y servicios
- Monitoreo de seguridad de red
- Desarrollo de herramientas
- Concientización
- Entrenamiento

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Nuestro rol en la UNLP

UNIVERSIDAD NACIONAL DE LA PLATA

Somos un grupo que trabaja en el ámbito de la Universidad Nacional de La Plata:

- Operando el CSIRT académico CERTUNLP.

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

CeSPI
UNIVERSIDAD NACIONAL DE LA PLATA

UNIVERSIDAD NACIONAL DE LA PLATA

- Realizando docencia, investigación y extensión en la Facultad de Informática.

PKIUNLP
Grid

CÁTEDRAS DE GRADO

SYPER
Cátedra de Grado y Postgrado

REDES Y SERVICIOS
Avanzadoso en Internet

DSA
Desarrollo Seguro de Aplicaciones

TLP:WHITE

Disclosure is not limited.

Origen de ScrubUNLP

UNIVERSIDAD NACIONAL DE LA PLATA

En las cátedras de grado y postgrado, se probaron con alumnos distintos mecanismos relacionados con BGP:

- RTBH (Remote trigger black hole)
- Servicio tipo UTRS de Team Cymru
- Ataques de tipo MITM utilizando BGP

ScrubUNLP es:

- una solución empaquetada de Scrubbing Center.
- Se diseñó como trabajo final para un grupo de estudiantes avanzados que trabajan en CERTUNLP.

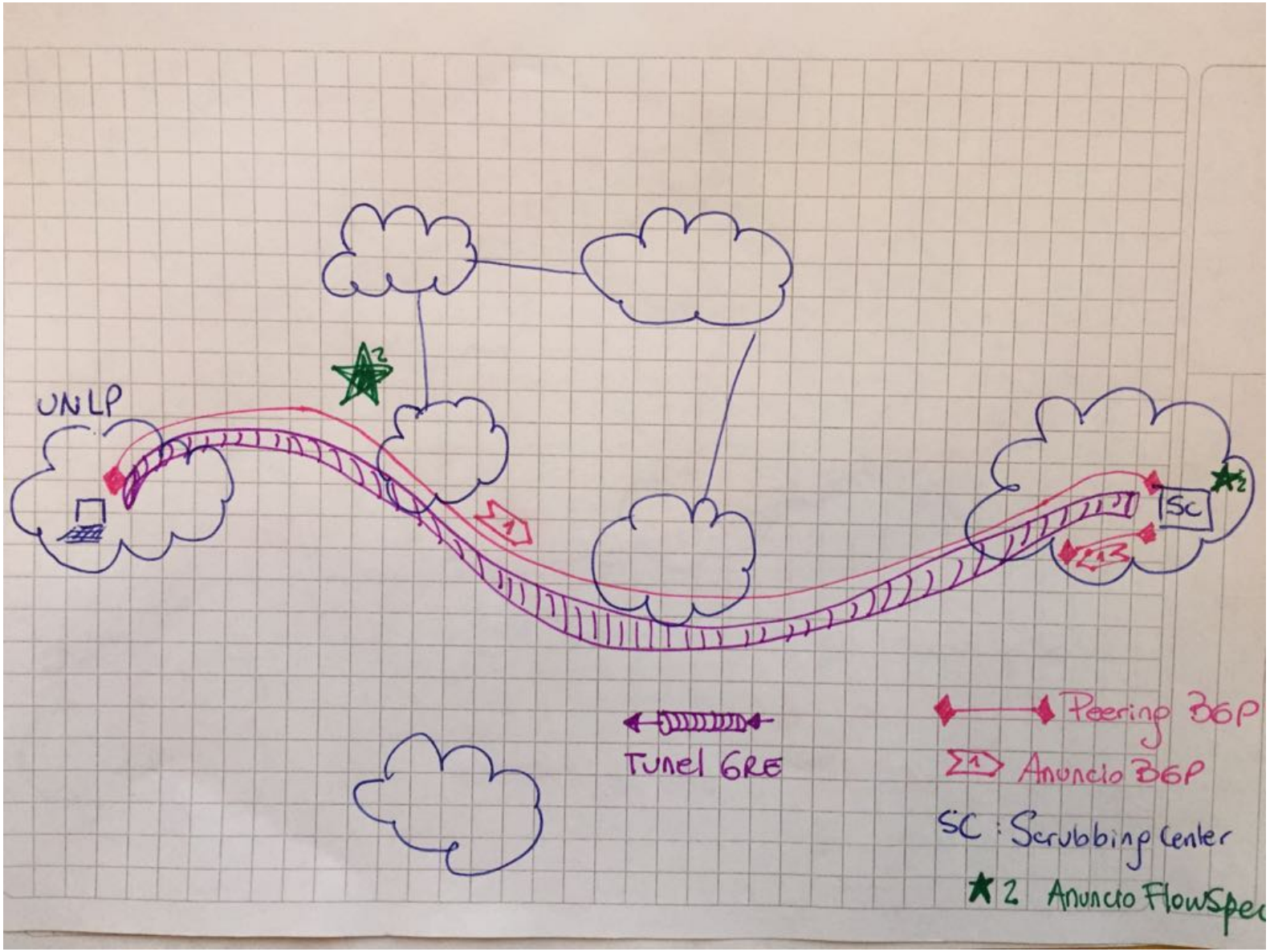
CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

ScrubUNLP - Diseño inicial

UNIVERSIDAD NACIONAL DE LA PLATA



CERT UNLP

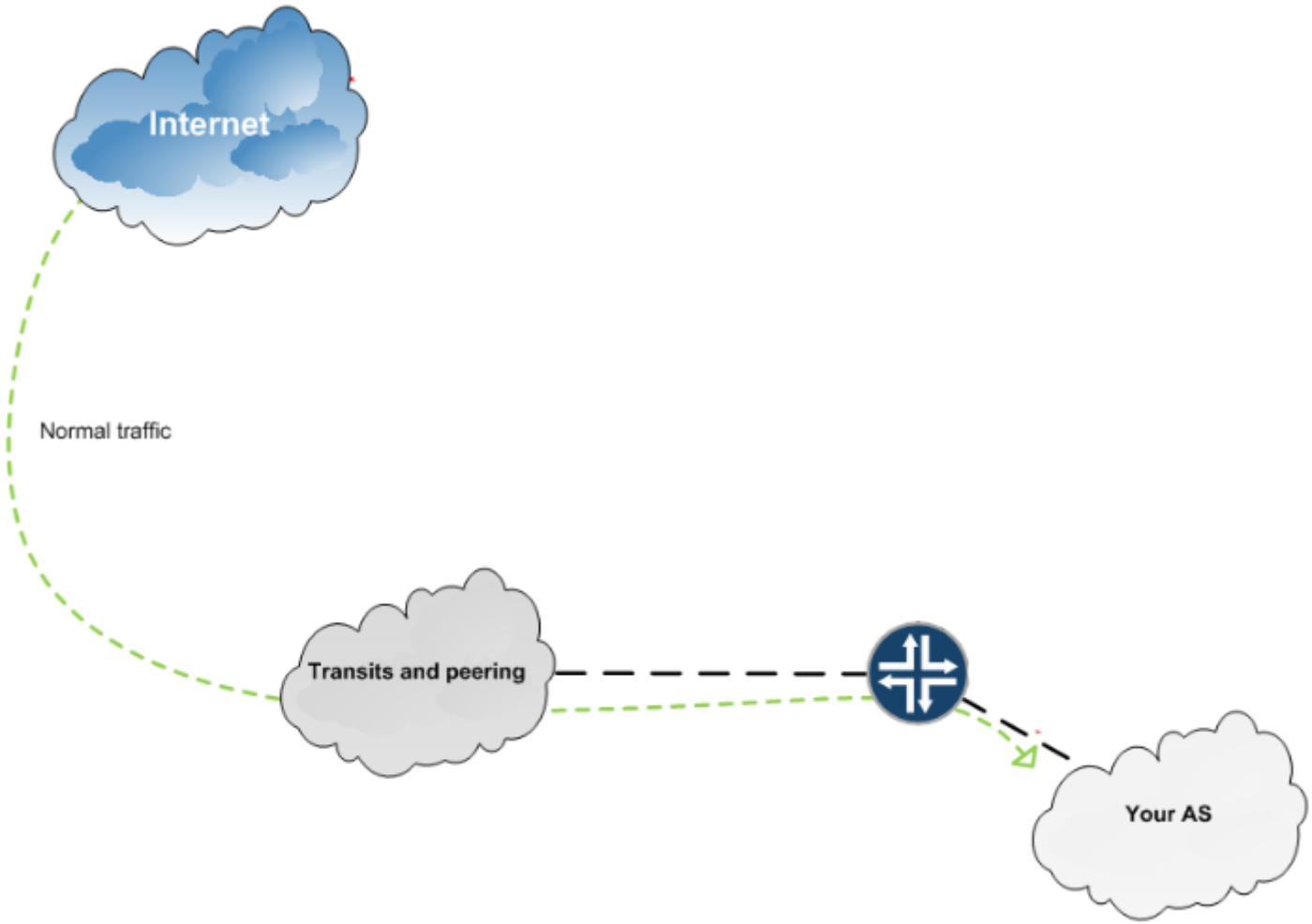
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Situación ideal

UNIVERSIDAD NACIONAL DE LA PLATA



CERT UNLP

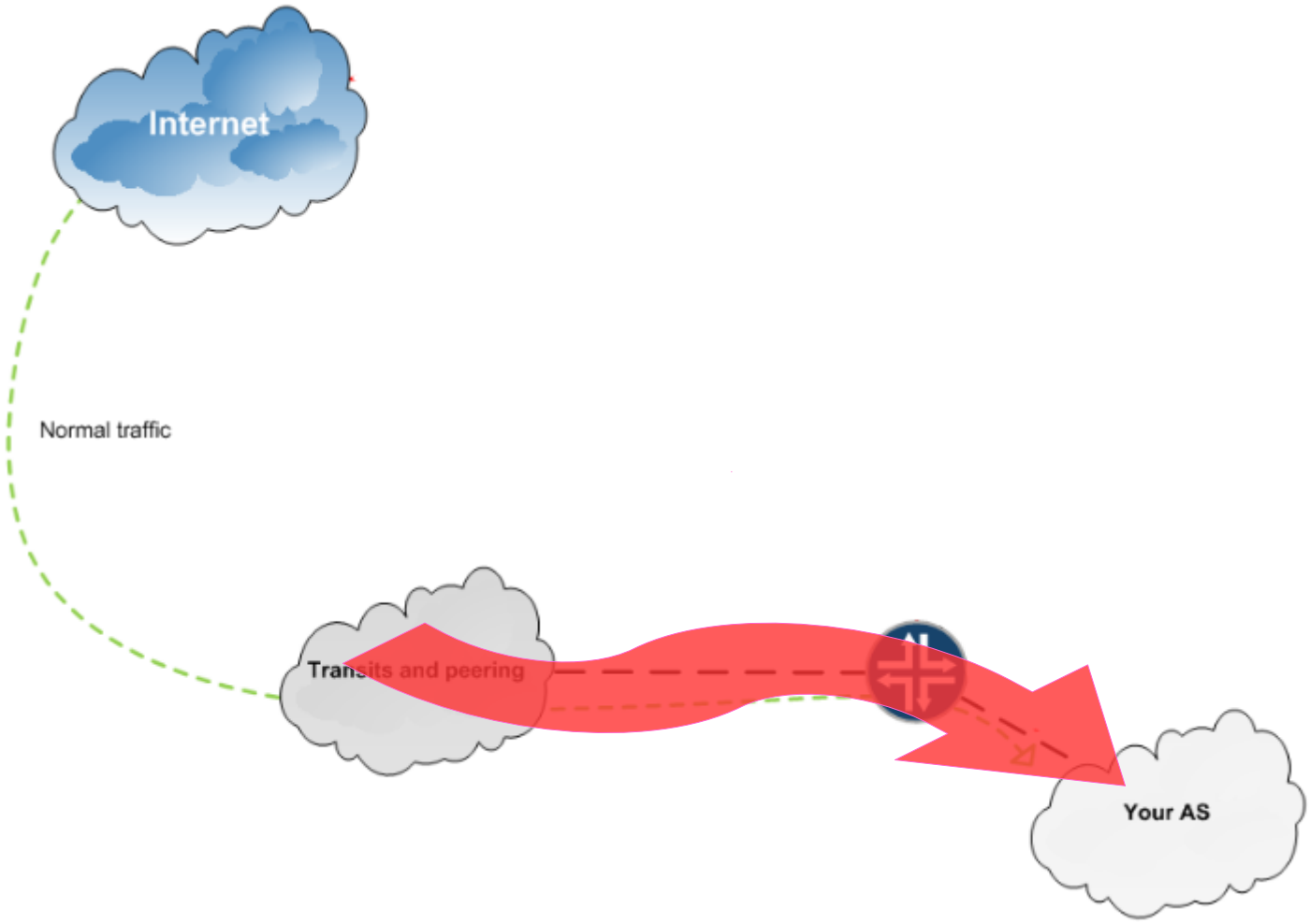
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Ataque DDoS volumétrico

UNIVERSIDAD NACIONAL DE LA PLATA



CERT UNLP

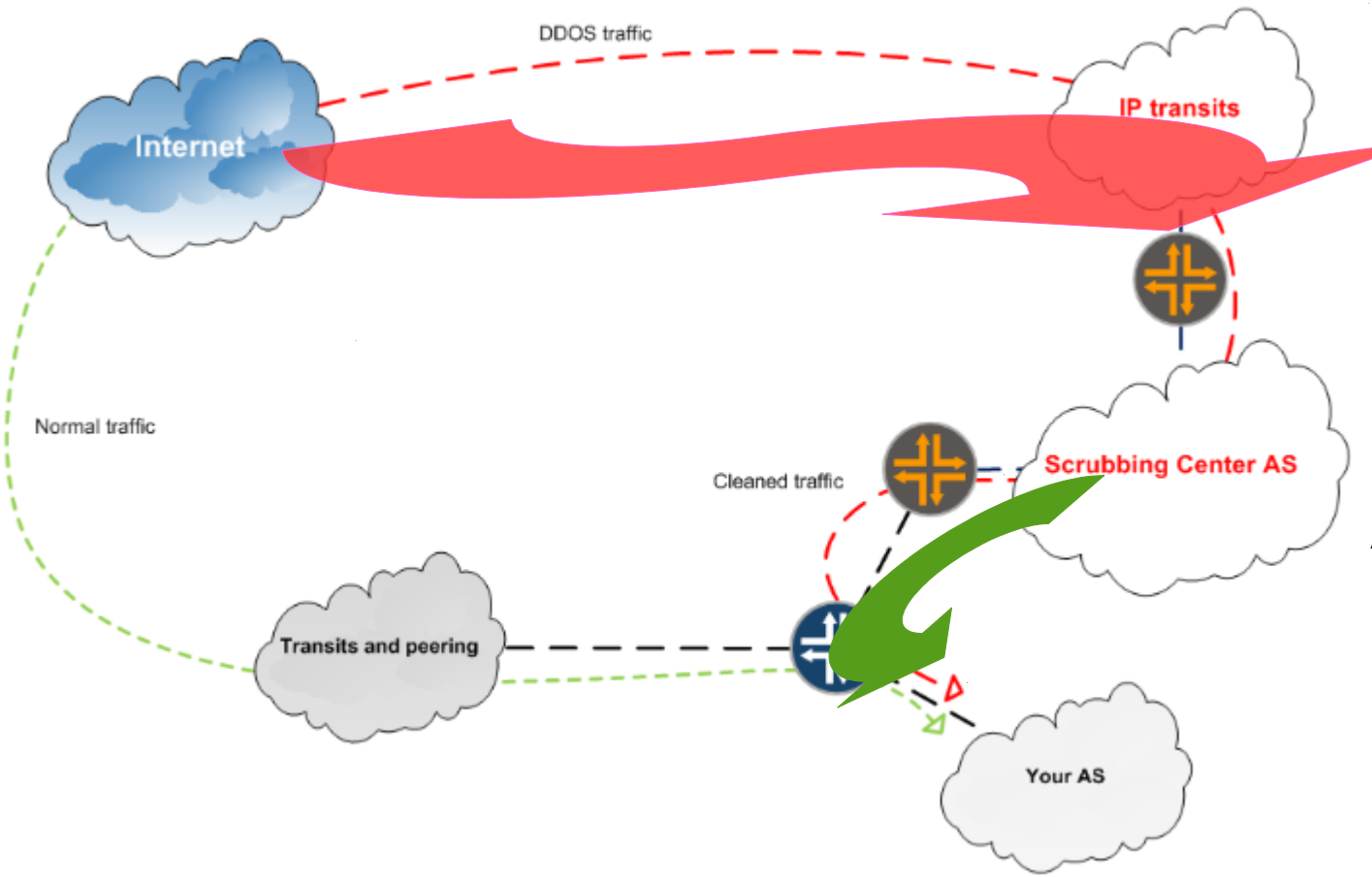
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Scrubbing Center

UNIVERSIDAD NACIONAL DE LA PLATA



El scrub center publica prefijos del cliente que están bajo ataque.

Esto evita que el ataque afecte las redes del cliente.

Además se limpia el tráfico para reenviar solamente aquello que no se considera malicioso.

CERT UNLP

Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Resumen Scrubbing Center

UNIVERSIDAD NACIONAL DE LA PLATA

- Un scrubbing center es un centro de limpieza de tráfico.
  - El tráfico es analizado y aquel considerado malicioso es eliminado antes de ser enviado a los clientes.
  - Se considera tráfico malicioso a aquel relacionado con DDoS, exploits, vulnerabilidades, etc.

- Empresas con peering en distintos países con múltiples proveedores son los principales oferentes de este tipo de servicio.

TLP:WHITE

Disclosure is not limited.

ScrubUNLP

UNIVERSIDAD NACIONAL DE LA PLATA

- Es un servicio de mitigación de DDoS.
- Fue implementado por CERTUNLP utilizando herramientas y tecnologías Open Source.
- Permite a los clientes:
  - Anunciar los bloques IP atacados, preservando el AS de origen.
  - Disponer de políticas de filtrado por defecto:
    - Bogons, DROP list, Port 19/udp, etc.
  - Indicar políticas de filtrado específicas para el cliente. Esto se realiza mediante anuncios FlowSpec

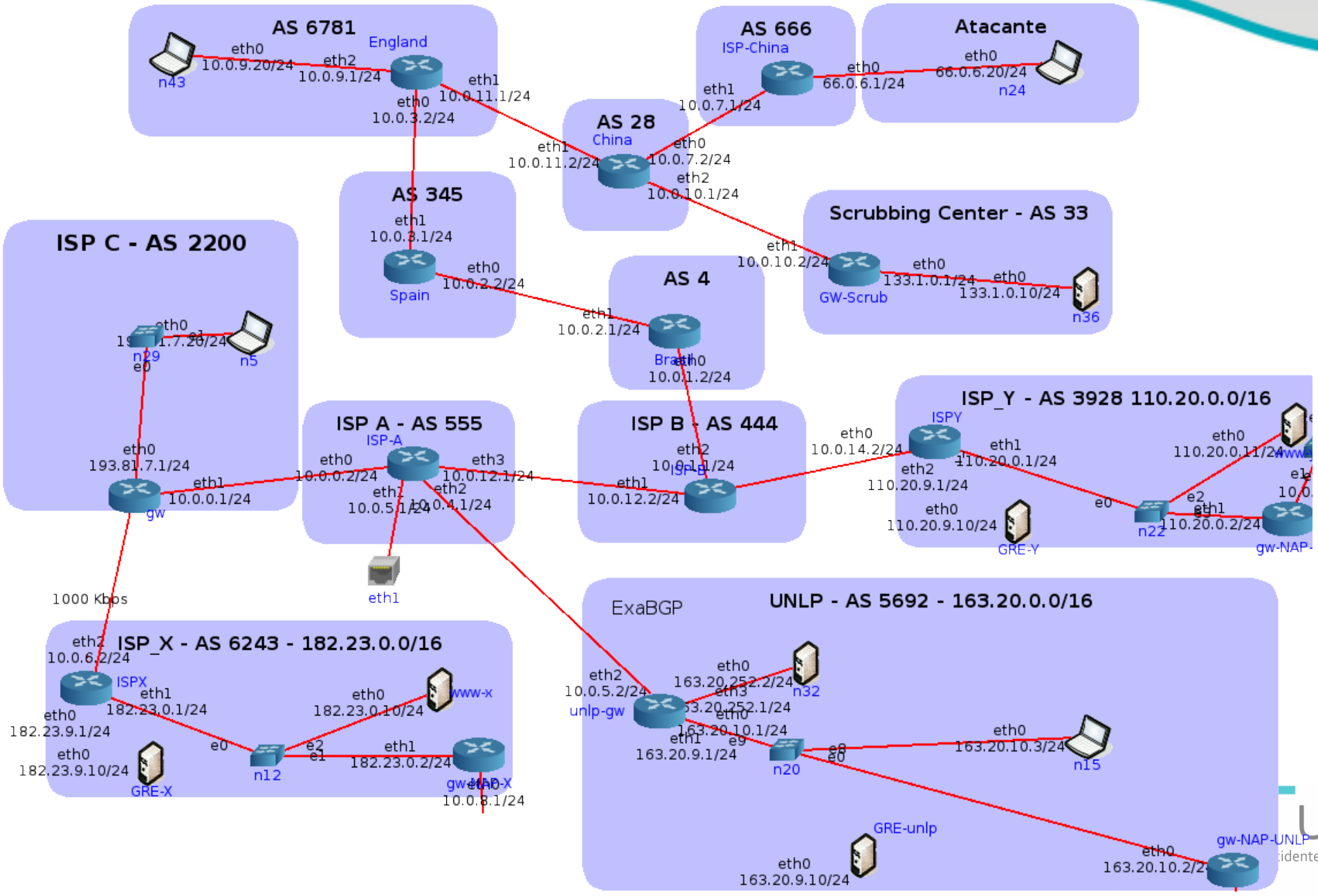
CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Maqueta de pruebas

UNIVERSIDAD NACIONAL DE LA PLATA



UNLP

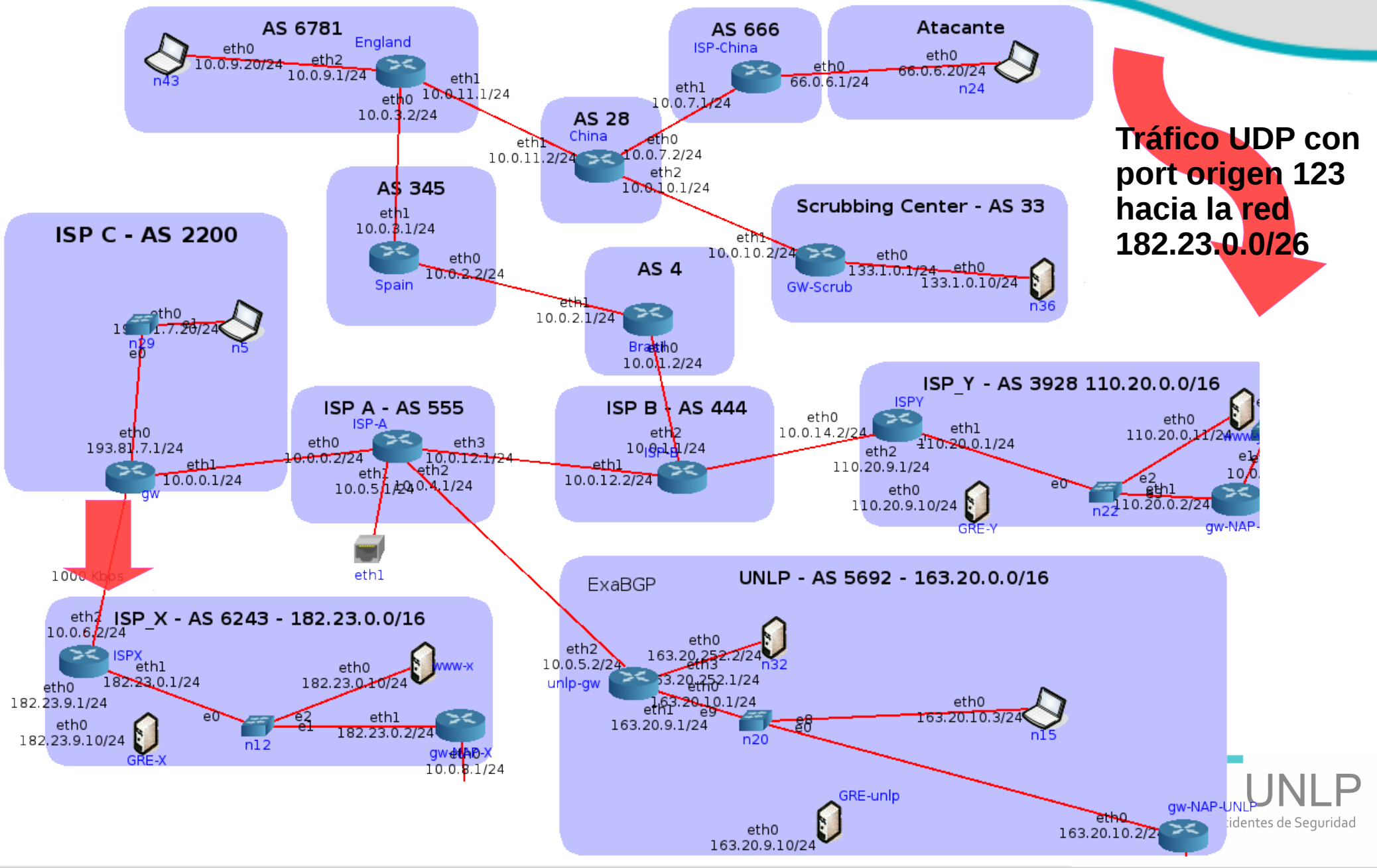
Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Ataque de DDoS
x ej: Reflexión NTP Monlist

UNIVERSIDAD NACIONAL DE LA PLATA



UNLP

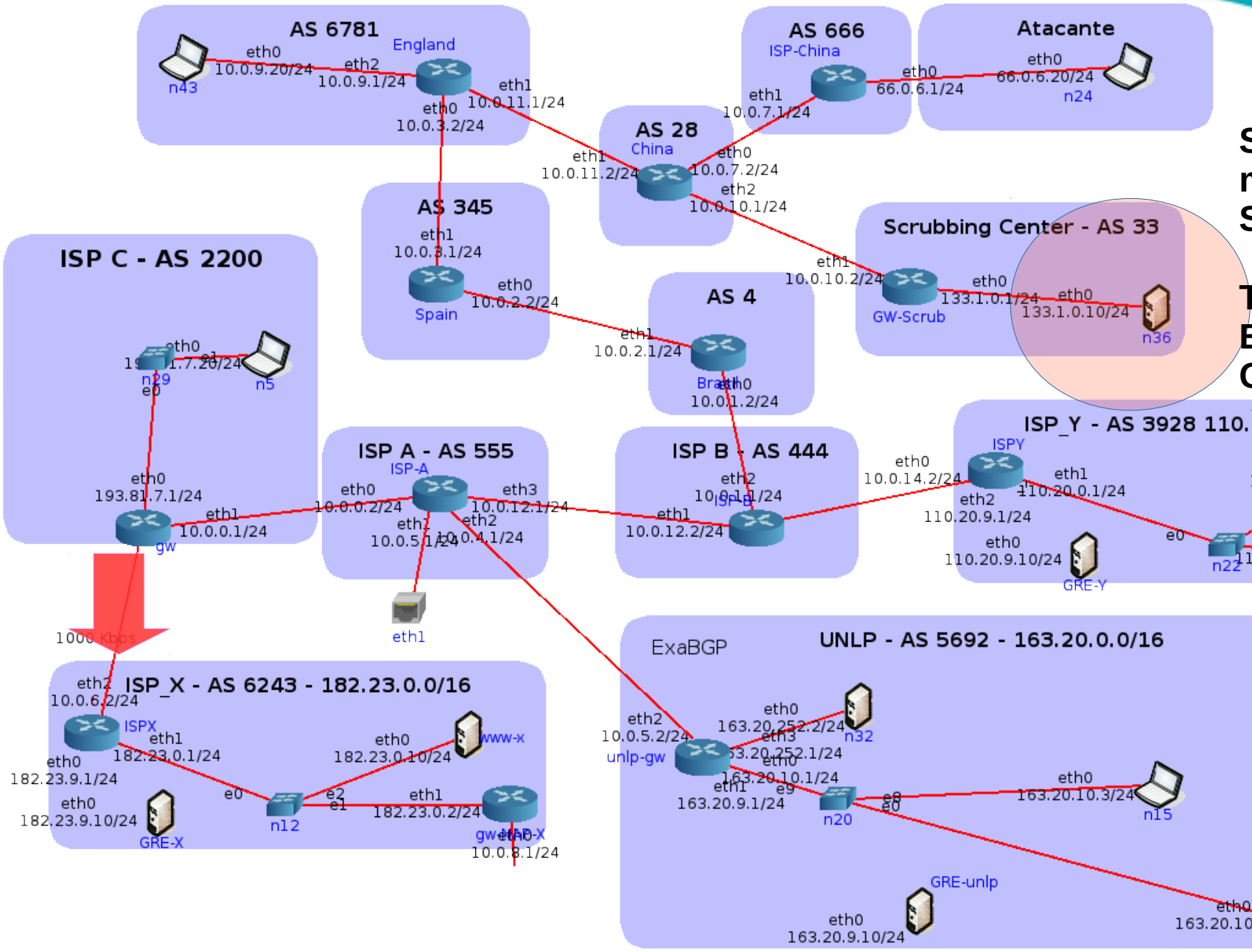
Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Scrubbing Center en la nube

UNIVERSIDAD NACIONAL DE LA PLATA



ScrubbingCenter manejado por ScrubUNLP

Tiene peering BGP contra GW-Scrub

UNLP

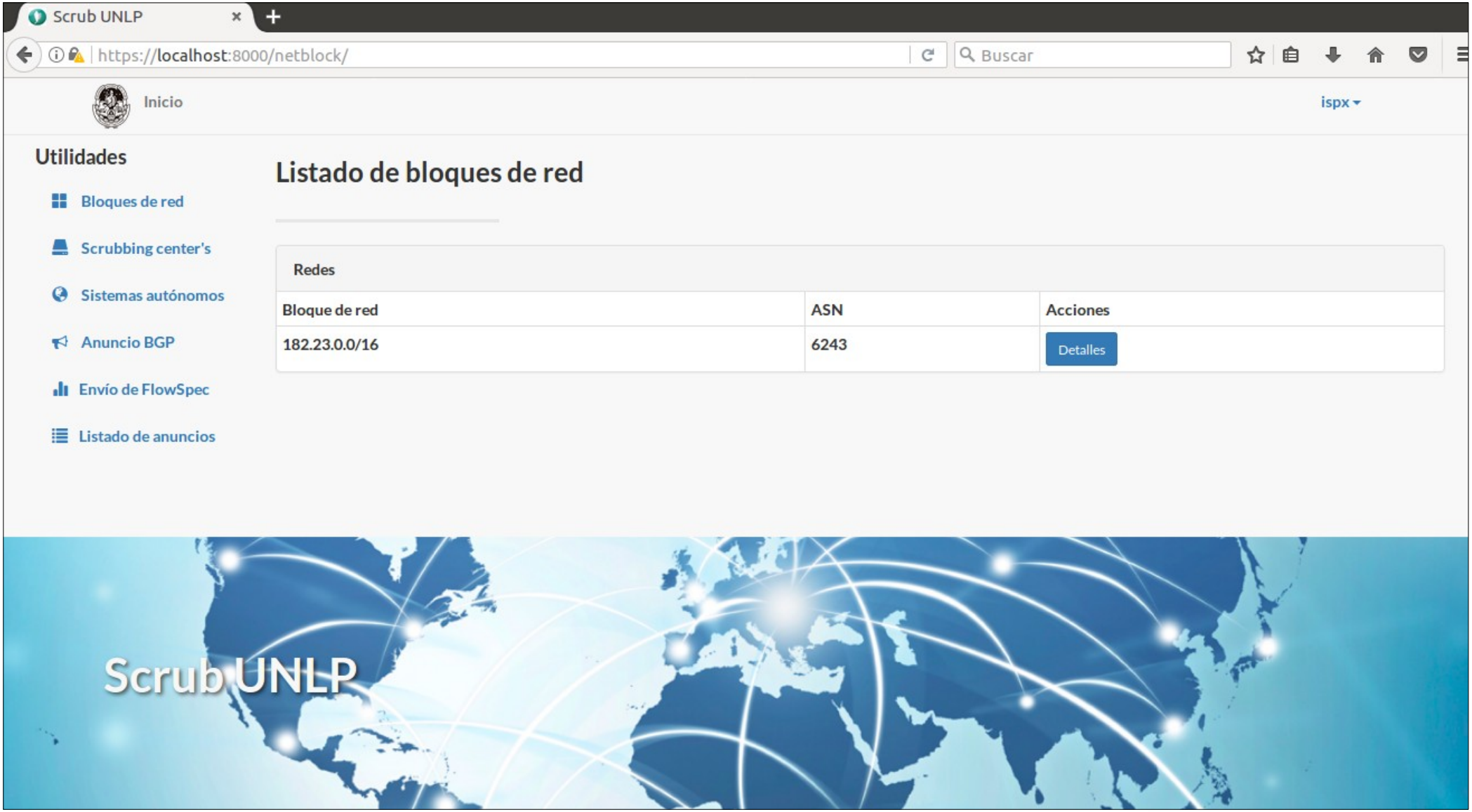
Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Consola de control de ScrubUNLP

UNIVERSIDAD NACIONAL DE LA PLATA

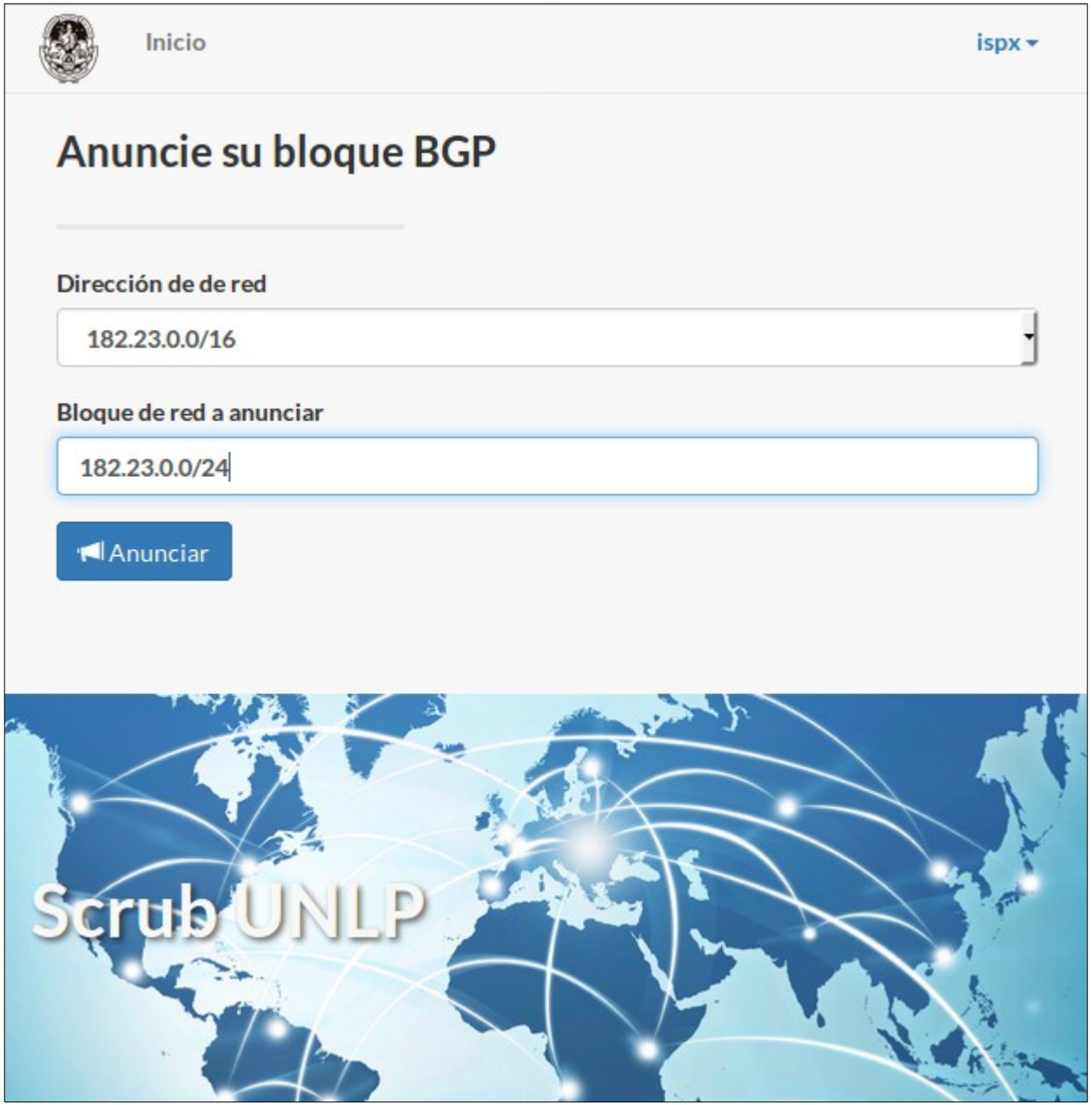


TLP:WHITE

Disclosure is not limited.

Anuncio ruta en Scrubbing Center

UNIVERSIDAD NACIONAL DE LA PLATA



CERT UNLP

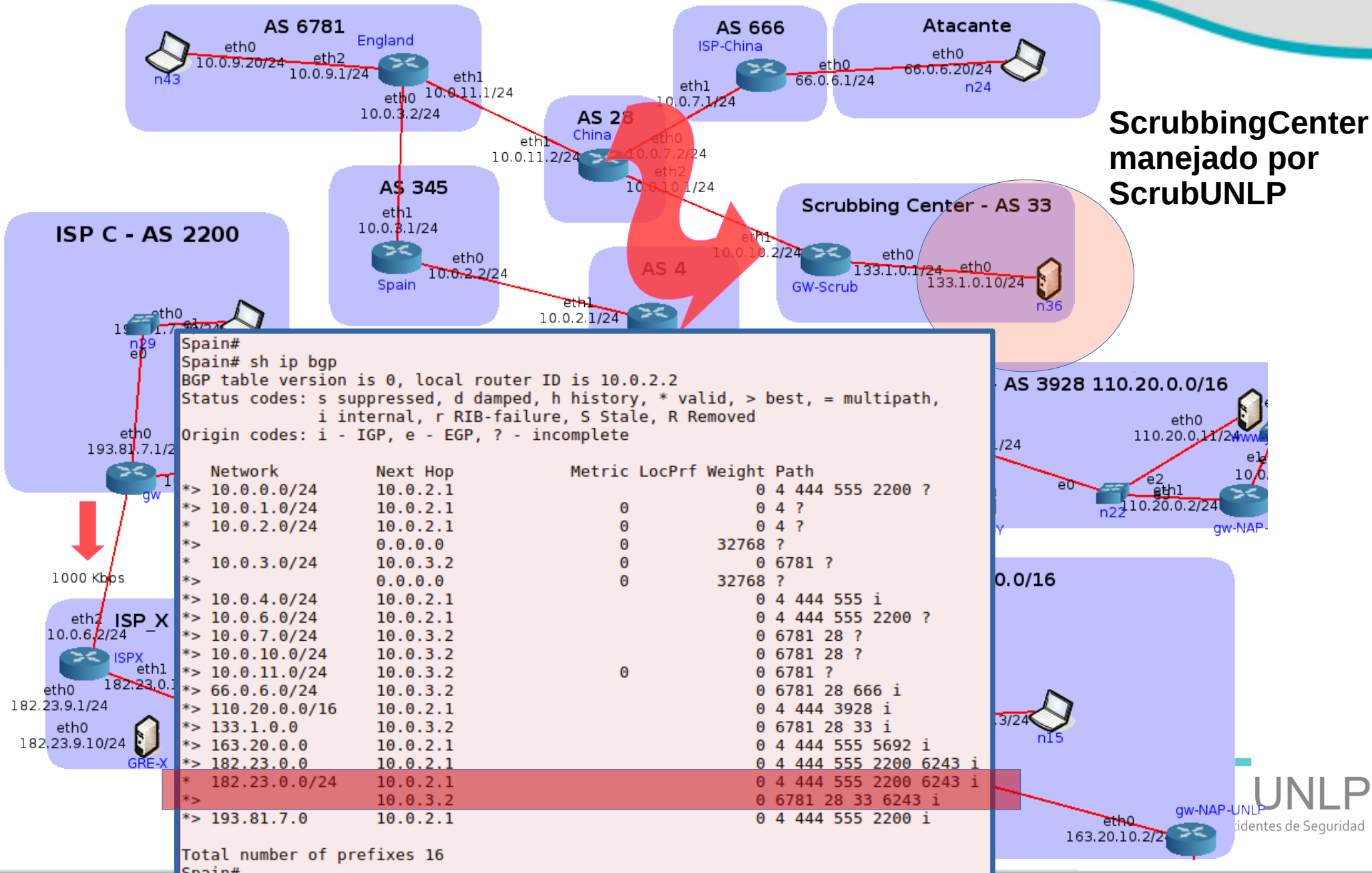
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

RTBH (Remote Trigger Black Hole) vs Limpieza de tráfico

UNIVERSIDAD NACIONAL DE LA PLATA




```
Spain#
Spain# sh ip bgp
BGP table version is 0, local router ID is 10.0.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0/24      10.0.2.1                               0 4 444 555 2200 ?
*> 10.0.1.0/24      10.0.2.1                 0             0 4 ?
*  10.0.2.0/24      10.0.2.1                 0             0 4 ?
*>                  0.0.0.0                  0         32768 ?
*  10.0.3.0/24      10.0.3.2                 0             0 6781 ?
*>                  0.0.0.0                  0         32768 ?
*> 10.0.4.0/24      10.0.2.1                               0 4 444 555 i
*> 10.0.6.0/24      10.0.2.1                               0 4 444 555 2200 ?
*> 10.0.7.0/24      10.0.3.2                               0 6781 28 ?
*> 10.0.10.0/24     10.0.3.2                               0 6781 28 ?
*> 10.0.11.0/24     10.0.3.2                 0             0 6781 ?
*> 66.0.6.0/24      10.0.3.2                               0 6781 28 666 i
*> 110.20.0.0/16    10.0.2.1                               0 4 444 3928 i
*> 133.1.0.0        10.0.3.2                               0 6781 28 33 i
*> 163.20.0.0       10.0.2.1                               0 4 444 555 5692 i
*> 182.23.0.0       10.0.2.1                               0 4 444 555 2200 6243 i
*  182.23.0.0/24    10.0.2.1                               0 4 444 555 2200 6243 i
*>                  10.0.3.2                               0 6781 28 33 6243 i
*> 193.81.7.0       10.0.2.1                               0 4 444 555 2200 i

Total number of prefixes 16
Spain#
```

ScrubbingCenter manejado por ScrubUNLP

UNLP

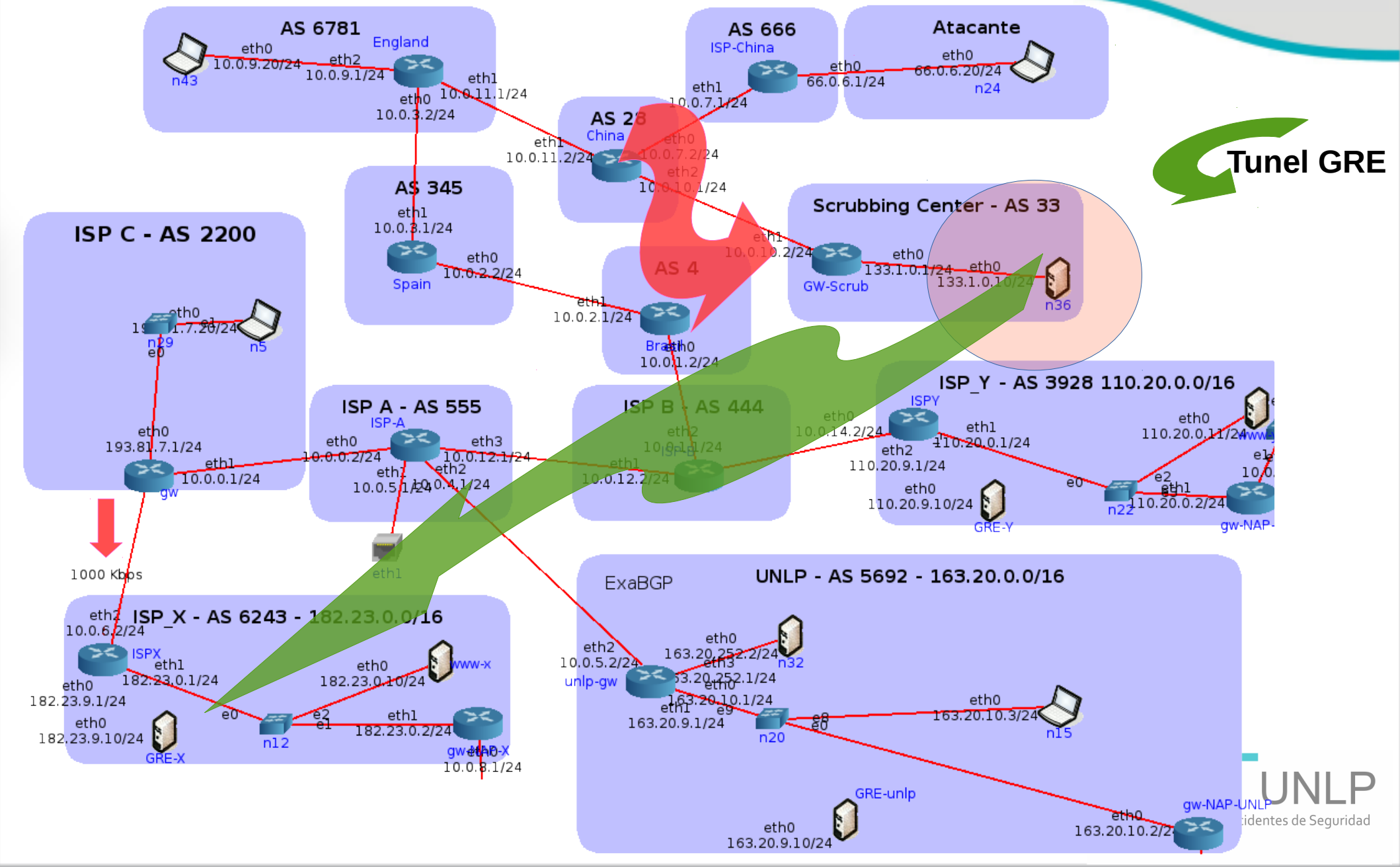
Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Limpieza de tráfico en Scrubbing Center

UNIVERSIDAD NACIONAL DE LA PLATA



UNLP

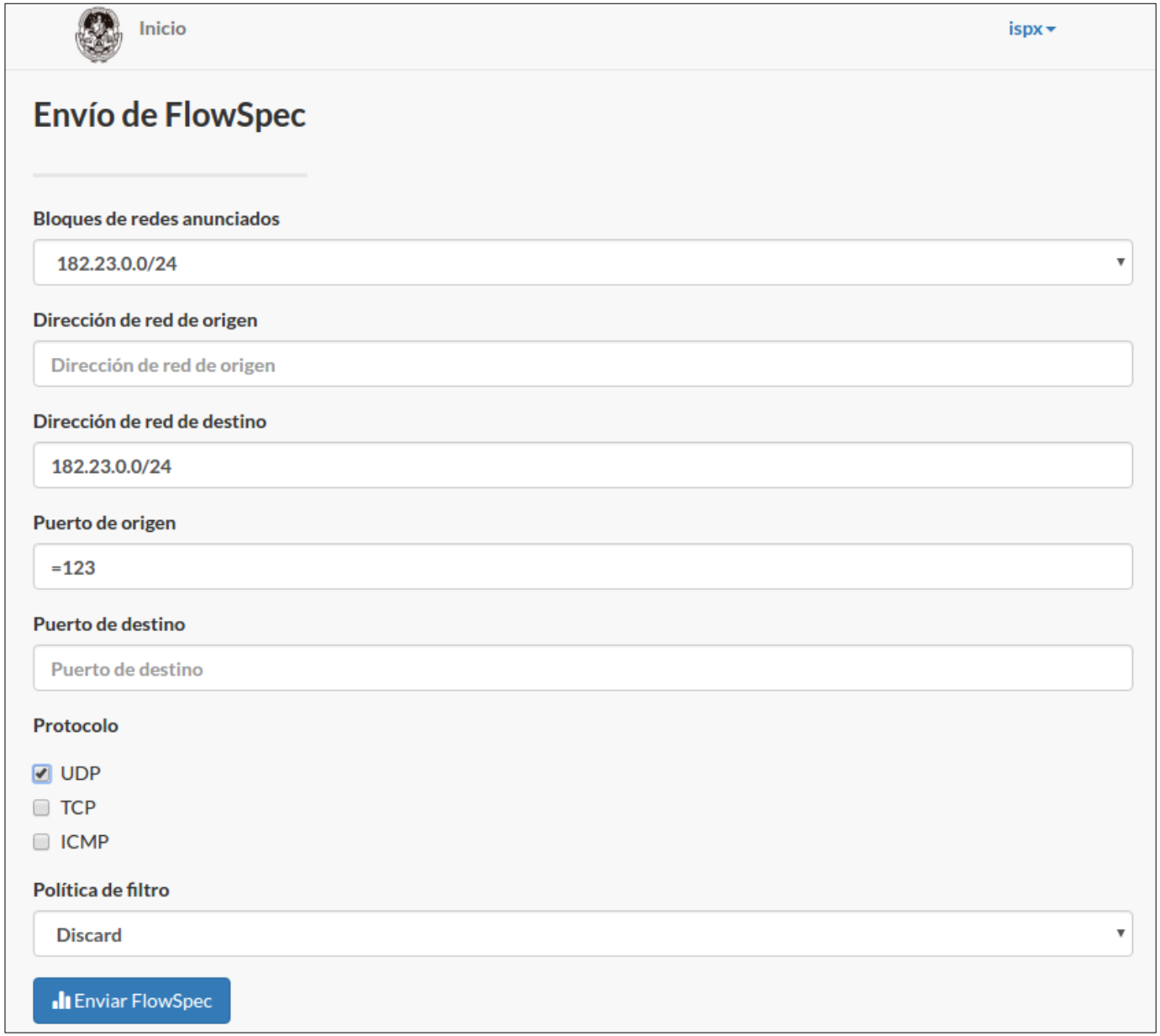
Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

FlowSpec para filtrar Reflexión NTP Monlist

UNIVERSIDAD NACIONAL DE LA PLATA



CERT UNLP

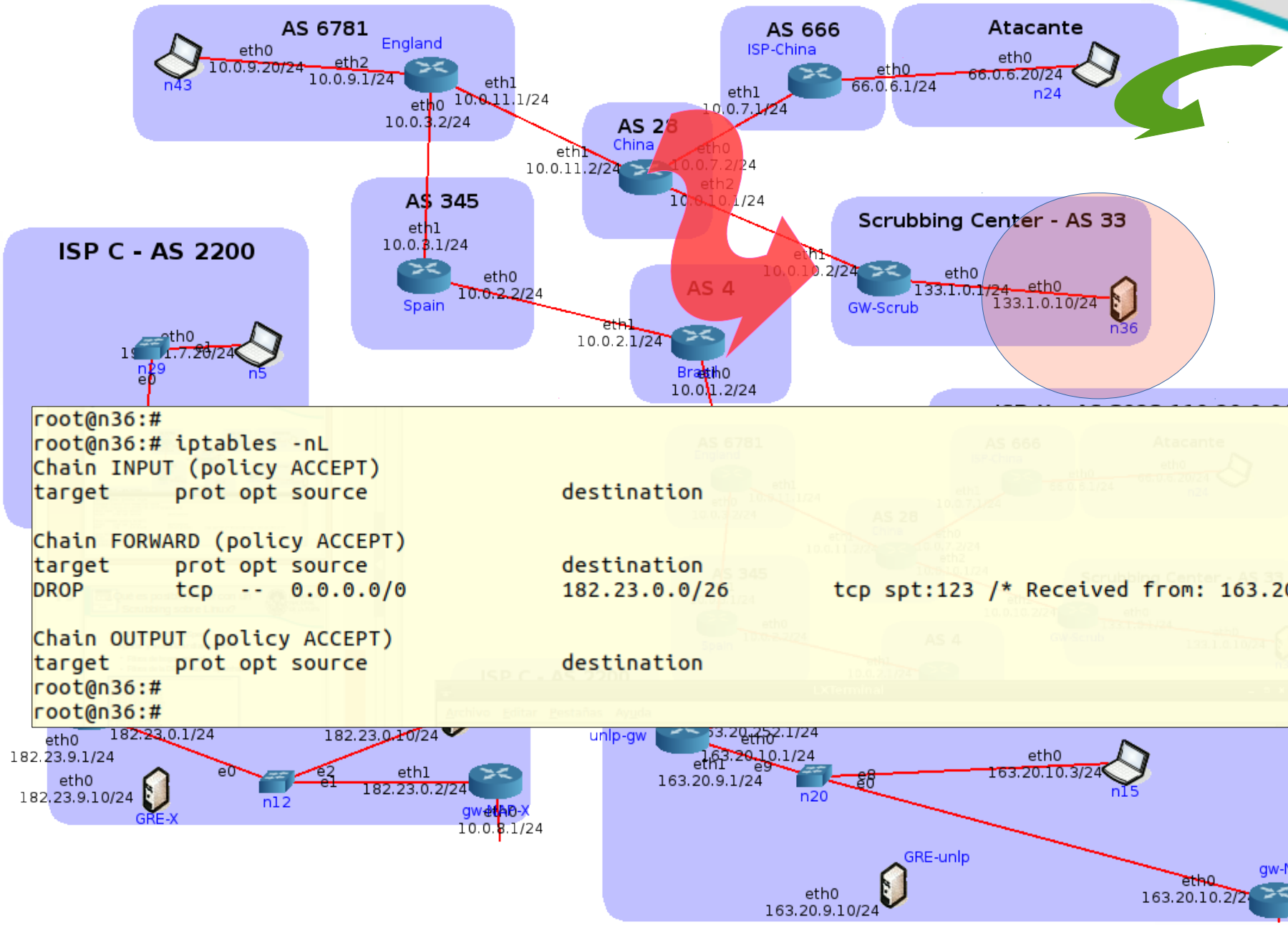
Equipo de Respuesta a Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

Anuncio de FlowSpec

UNIVERSIDAD NACIONAL DE LA PLATA



UNLP

Incidentes de Seguridad

TLP:WHITE

Disclosure is not limited.

¿Qué es posible hacer con un Scrubbing sobre Linux?

UNIVERSIDAD NACIONAL DE LA PLATA

- Aplicar filtros FlowSpec bajo demanda del cliente
- Aplicar y actualizar filtros predeterminados:
  - Filtros de bogon networks
  - Filtros de la DROP List de Spamhaus

```
INFO: Descargando Bogons IPv4 de TeamCymru (http://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt).

INFO: Analizando datos en nethash bogons_ipv4.
INFO: Eliminando 45.6.76.0/22 de bogons_ipv4.
INFO: Eliminando 45.6.80.0/20 de bogons_ipv4.
INFO: Eliminando 45.6.96.0/19 de bogons_ipv4.
INFO: Eliminando 103.89.68.0/22 de bogons_ipv4.
INFO: Eliminando 103.89.72.0/21 de bogons_ipv4.
INFO: Eliminando 103.89.80.0/20 de bogons_ipv4.
INFO: Eliminando 103.89.96.0/19 de bogons_ipv4.
INFO: Eliminando 116.206.144.0/20 de bogons_ipv4.
INFO: Eliminando 116.206.160.0/19 de bogons_ipv4.
INFO: Eliminando 185.197.28.0/22 de bogons_ipv4.
INFO: Eliminando 185.197.32.0/19 de bogons_ipv4.
INFO: Eliminando 185.197.64.0/18 de bogons_ipv4.
INFO: Agregando 45.6.102.0/23 a bogons_ipv4.
INFO: Agregando 45.6.104.0/21 a bogons_ipv4.
INFO: Agregando 45.6.112.0/20 a bogons_ipv4.
INFO: Agregando 103.89.73.0/24 a bogons_ipv4.
INFO: Agregando 103.89.74.0/23 a bogons_ipv4.
INFO: Agregando 116.206.168.0/21 a bogons_ipv4.
INFO: Agregando 116.206.176.0/20 a bogons_ipv4.
INFO: Agregando 185.197.88.0/21 a bogons_ipv4.
INFO: Agregando 185.197.96.0/19 a bogons_ipv4.

INFO: Actualizando archivo /home/cert/ipset2/lists/list_ipv4.txt.


INFO: Descargando droplist de Spamhaus (https://www.spamhaus.org/drop/drop.txt).

INFO: Analizando datos en nethash droplist.
INFO: Eliminando 1.116.0.0/14 de droplist.

INFO: Actualizando archivo /home/cert/ipset2/lists/list_droplist.txt.
```

CERT UNLP

Equipo de Respuesta a Incidentes de Seguridad

Scrubbing Center sobre Linux

- Alternativamente se puede tener un router BGP con soporte FlowSpec – RFC 5575
- Sobre las técnicas de mitigación de DDoS:
  - Filtros predeterminados para comunicaciones de servicios que no deberían estar expuestos: SSDP, Chargen, Portmapper, NetBIOS.
  - Filtros en función del tamaño de los paquetes. (a futuro)
  - Filtros personalizados por cliente. (a futuro)
  - Implementación de rate-limit de tráfico, en especial filtros en función de la cantidad de paquetes enviados por una IP o bloque /24. (a futuro)

TLP:WHITE

Disclosure is not limited.

UNIVERSIDAD NACIONAL DE LA PLATA

CERTUNLP

Universidad **N**acional de **L**a **P**lata

Contacto: info@cert.unlp.edu.ar

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad