Cuando el cielo se cae

Mitigación a escala de red de los ataques DDoS de reflexión/amplificación de gran volumen

Roland Dobbins rdobbins@arbor.net
Ingeniero principal, ASERT

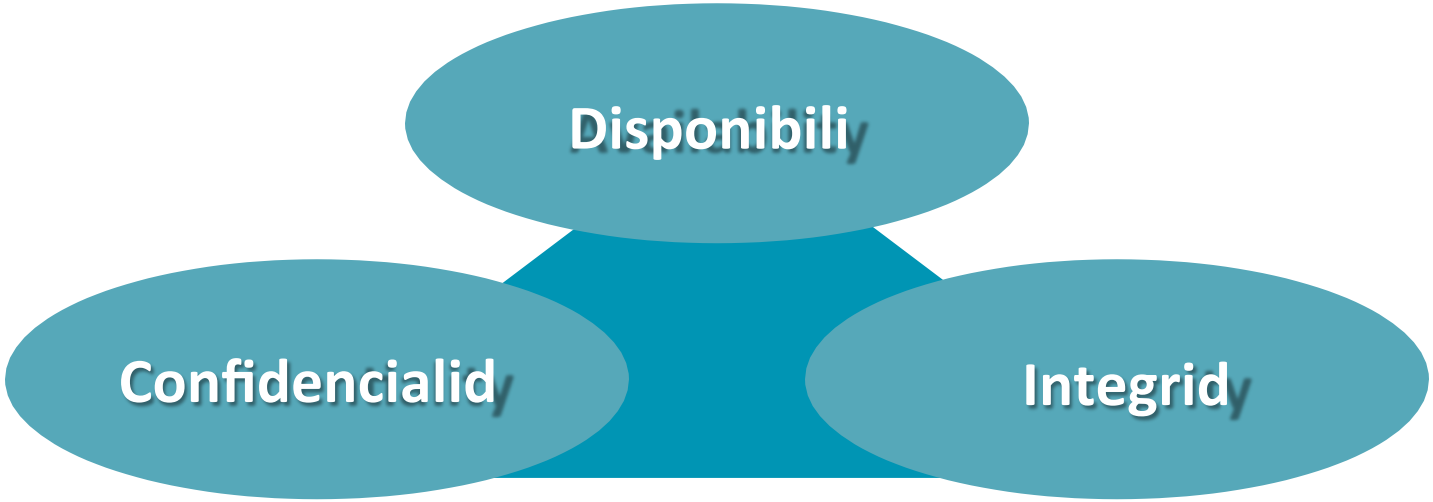
Introducción & Contexto

Antecedentes del DDoS

¿Qué es un ataque de denegación de servicio distribuido (DDoS)?

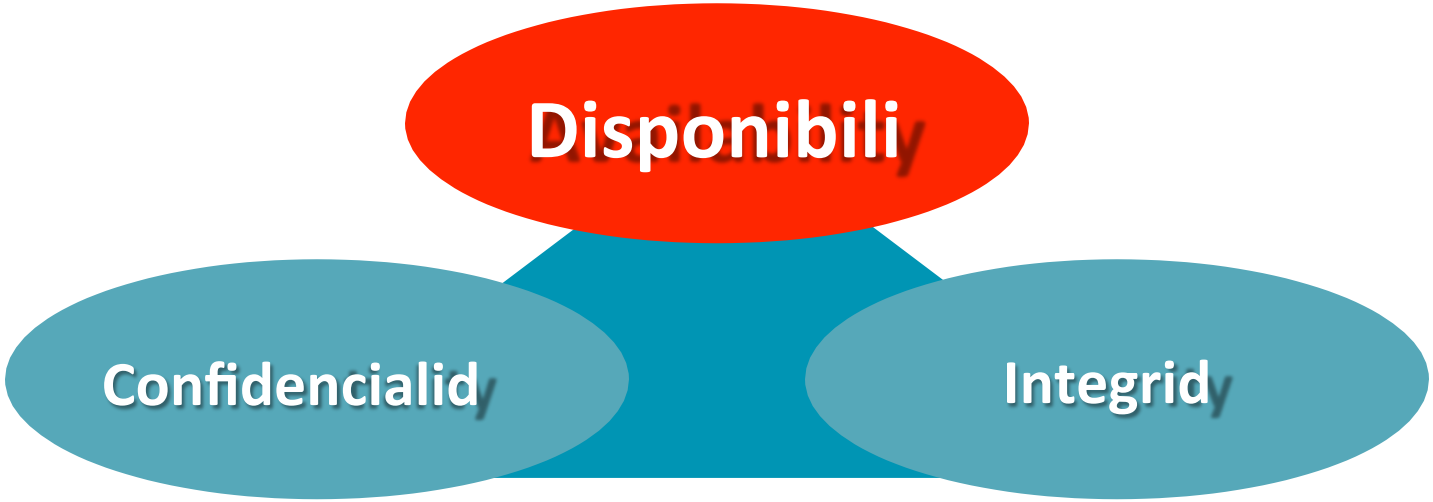
- Un intento de **consumir recursos** finitos, **explotar las debilidades** del diseño o la implementación del software, o **aprovechar la falta de capacidad de** la infraestructura
- Se centra en la **disponibilidad** y **utilidad** de los recursos informáticos y de red
- Los ataques casi siempre se **distribuyen** para lograr un efecto aún más significativo (es decir, DDoS)
- Los **daños colaterales** causados por un ataque pueden ser tan graves, o incluso peores, que el propio ataque
- **Los ataques DDoS afectan a la disponibilidad¡Sin** disponibilidad no applications/services/ data/Internet! no hay ingresos!
- **Los** ataques DDoS son ataques **contra la capacidad y/o el estado**.

Tres características de seguridad



- El objetivo de la seguridad es mantener estas tres características

Tres características de seguridad



- El objetivo principal de la defensa DDoS es mantener la disponibilidad frente a los ataques

Casi todo el gasto/esfuerzo en seguridad se centra en la confidencialidad y la integridad

- La confidencialidad y la integridad son conceptos relativamente sencillos, fáciles de entender para los no especialistas
- En la práctica, la confidencialidad y la integridad equivalen prácticamente a la encriptación.
- La realidad es que hay algo más que la encriptación, pero es fácil proclamar la victoria: "Tenemos antivirus, tenemos encriptación de disco, cumplimos con la PCI, ¡woo- hoo! "
- Y sin embargo, cientos de millones de hosts bots; redes empresariales de todos los tamaños en todos los verticales completamente penetradas, propiedad intelectual robada, secretos de defensa filtrados, etc.
- La disponibilidad no puede ser refinada - el servidor Web/Servidor DNS/PBX VoIP o está en funcionamiento o no lo está. No hay manera de ofuscar/exagerar/prevaricar con respecto a la postura de seguridad real del mundo.
- La disponibilidad requiere profesionales de la seguridad operativa (opsec) que comprendan TCP/IP y el enrutamiento/conmutación; que comprendan los servidores web; que comprendan los servidores DNS; que comprendan la seguridad; que comprendan la capa 7.
- Estas personas son raras y no son baratas. La mayoría de las organizaciones ni siquiera entienden las habilidades requeridas y el alcance de la experiencia que deben buscar para identificar y contratar a las personas adecuadas.

La disponibilidad es difícil.

- Mantener la disponibilidad frente a los ataques requiere una combinación de habilidades, arquitectura, agilidad operativa, capacidades analíticas y capacidades de mitigación que la mayoría de las organizaciones simplemente no poseen
- En la práctica, la mayoría de las organizaciones nunca tienen en cuenta la disponibilidad a la hora de diseñar/especificar/construir/desplegar/probar aplicaciones/servicios/propiedades en línea
- En la práctica, la mayoría de las organizaciones nunca establecen la conexión lógica entre el mantenimiento de la disponibilidad y la continuidad del negocio
- En la práctica, la mayoría de las organizaciones nunca hacen pruebas de estrés de sus pilas de aplicaciones/servicios para determinar las deficiencias de escalabilidad/resiliencia y proceder a solucionarlas
- En la práctica, la mayoría de las organizaciones no tienen planes de mitigación de DDoS - o si tienen un plan, ¡nunca lo ensayan!

Reflección/Amplificación de ataques DDoS

Evolución de los ataques DDoS de reflexión/amplificación

- Se han observado muchas variedades de ataques DDoS de reflexión/amplificación "en la naturaleza" durante **18 años o más.**
- A partir de octubre de 2013, se lanzaron ataques DDoS de reflexión/amplificación NTP de alto perfil contra varios servicios de **juego en línea**.
- Con **decenas de millones de usuarios simultáneos** afectados, estos ataques fueron reportados por la prensa tecnológica.
- Pero estos ataques no son nuevos: los **mayores ataques DDoS observados** son todos ataques de reflexión/amplificación, y **lo han sido durante años**.
- Los ataques de reflexión/amplificación requieren la capacidad de **falsificar la dirección IP** del objetivo previsto.
- bandwidth (bps). En la mayoría de los ataques DDoS volumétricos, el rendimiento (pps) es más **importante** que bandwidth (bps). En la mayoría de los ataques DDoS de reflexión/amplificación, **los bps son más importantes que los pps**: ¡llenan las tuberías!

Componentes de un ataque DDoS de reflexión/amplificación

Amplificación

- El atacante hace una petición relativamente pequeña que genera una respuesta/replica significativamente mayor. Esto ocurre con la mayoría de las respuestas del servidor (no todas).

Reflexión

- El atacante envía solicitudes falsas a un gran número de dispositivos conectados a Internet, que responden a las solicitudes. Mediante la suplantación de la dirección IP, la dirección "de origen" se establece en el objetivo real del ataque, donde se envían todas las respuestas. Muchos servicios pueden ser explotados para actuar como reflectores.

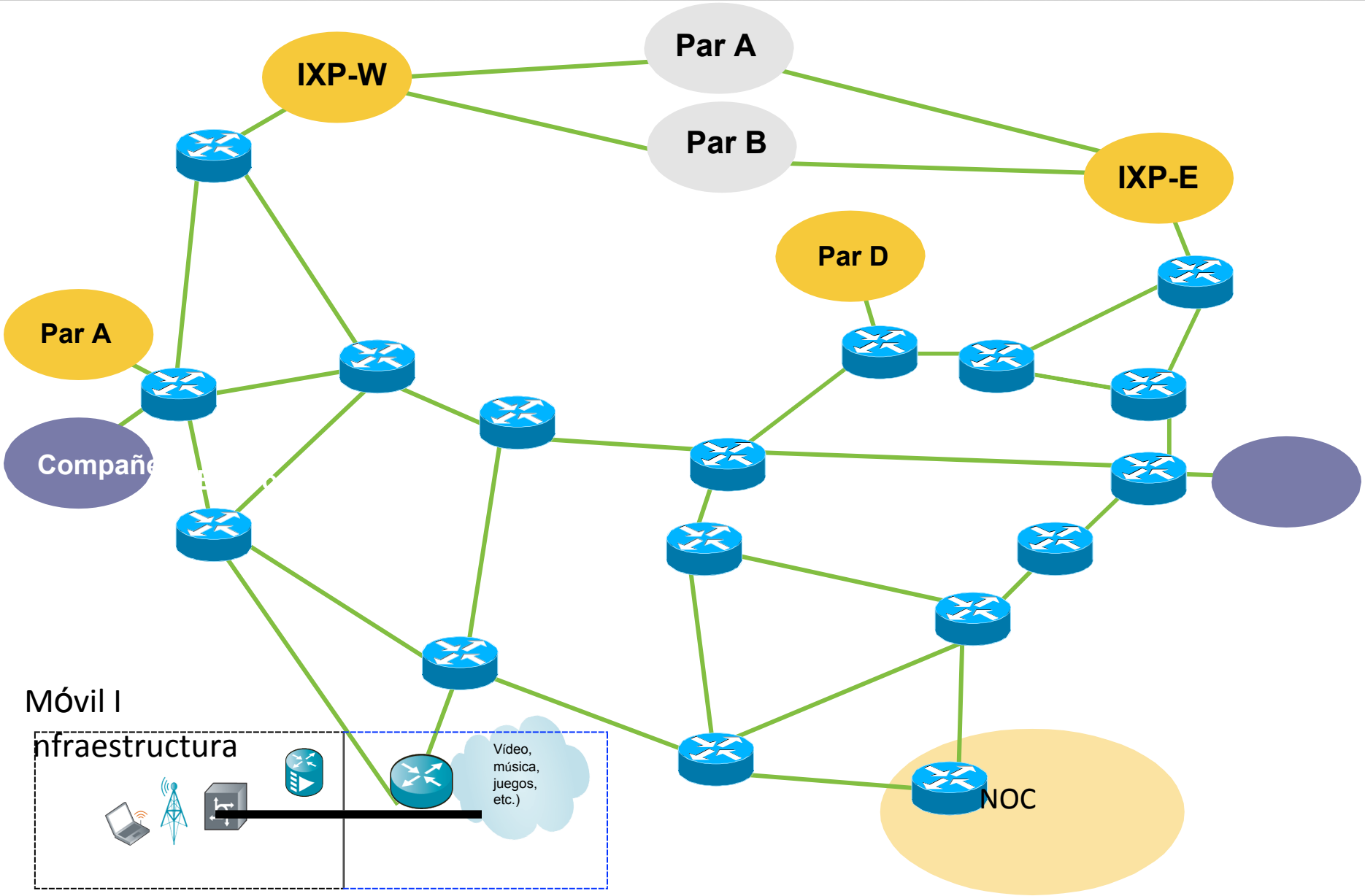
Impacto de los ataques DDoS de reflexión/amplificación

- Servidores, servicios, aplicaciones, acceso a Internet, etc., en la red de destino ***abrumados e indisponibles*** por el mero volumen de tráfico: decenas o cientos de gb/seg. frecuentes.
- ***Saturación completa*** de los enlaces de peering/tránsito de la red de destino.
- ***Saturación total o casi total*** de los enlaces de interconexión/tránsito/enlaces centrales de las redes intermedias entre los reflectores/amplificadores y la red de destino, incluidas las redes de los pares directos/proveedores de tránsito de la red de destino
- ***Daños colaterales generalizados***: pérdida de paquetes, retrasos, alta latencia para el tráfico de Internet de las partes no implicadas que simplemente atraviesan las redes saturadas por estos ataques.

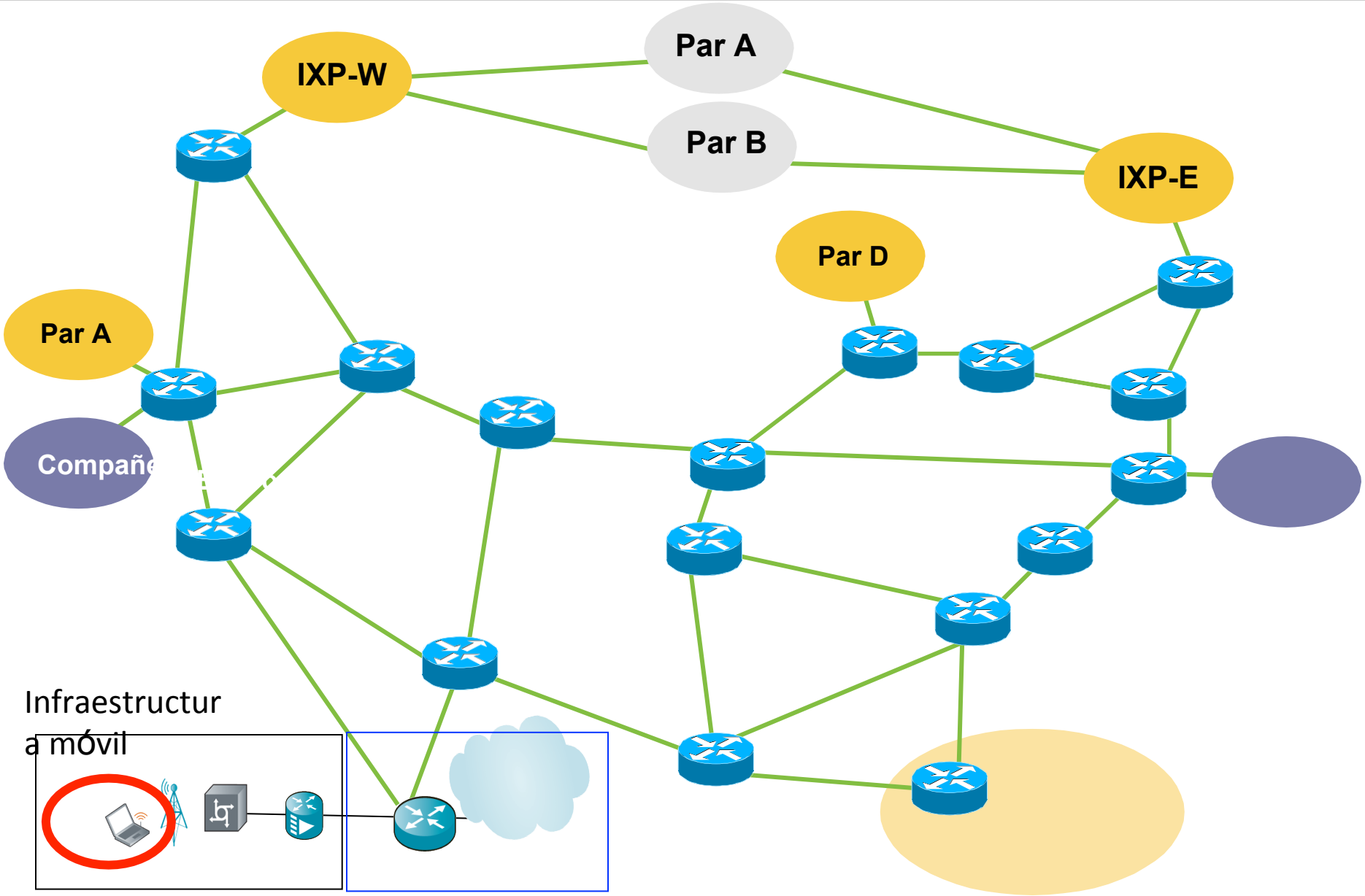
Impacto de los ataques DDoS de reflexión/amplificación

- ***Indisponibilidad*** de servidores/servicios/aplicaciones, acceso a Internet para transeúntes topológicamente próximos a la red objetivo.

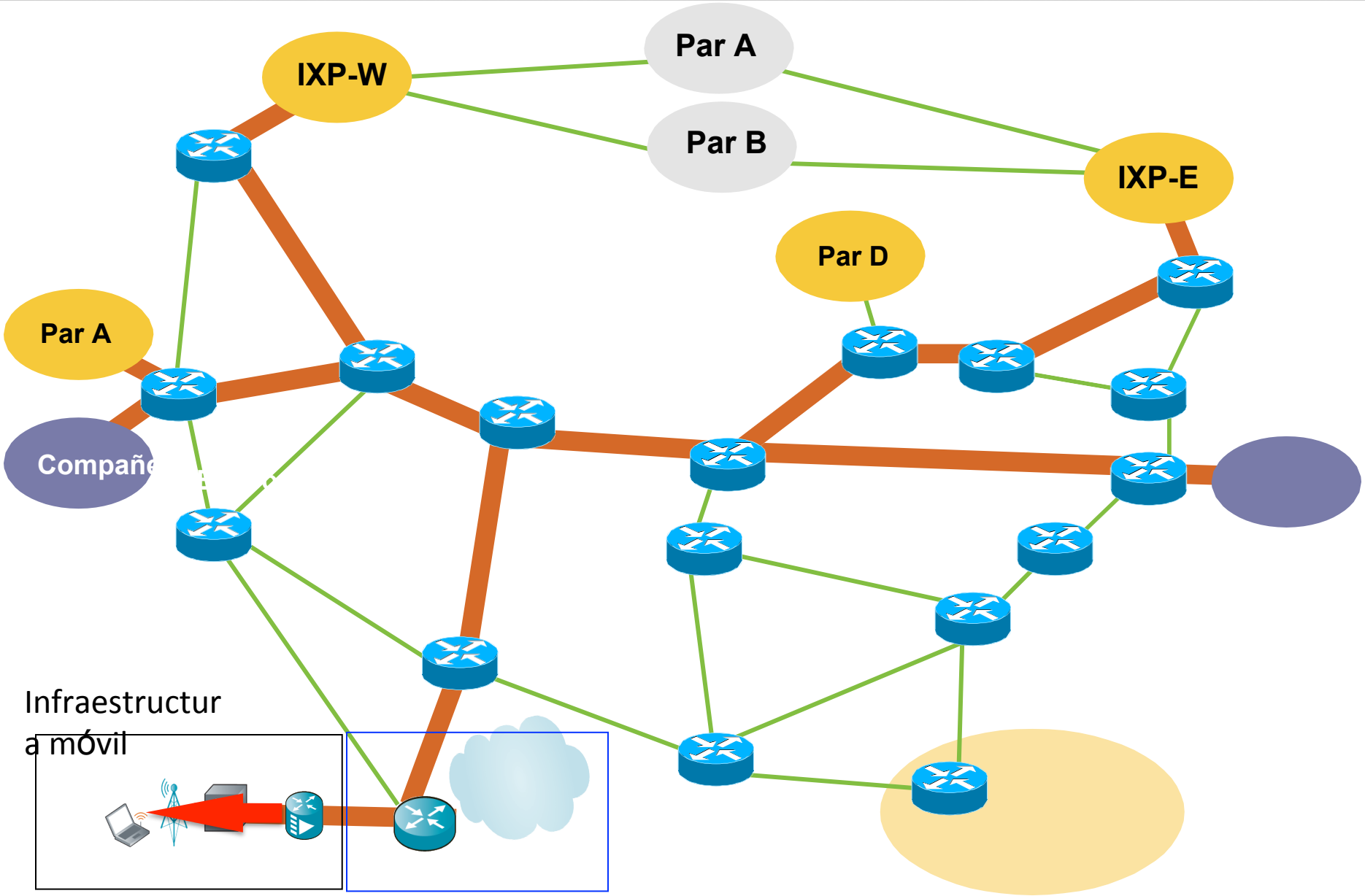
Efectos de un ataque DDoS de reflexión / amplificación de 400 gb/s en la capacidad de la red



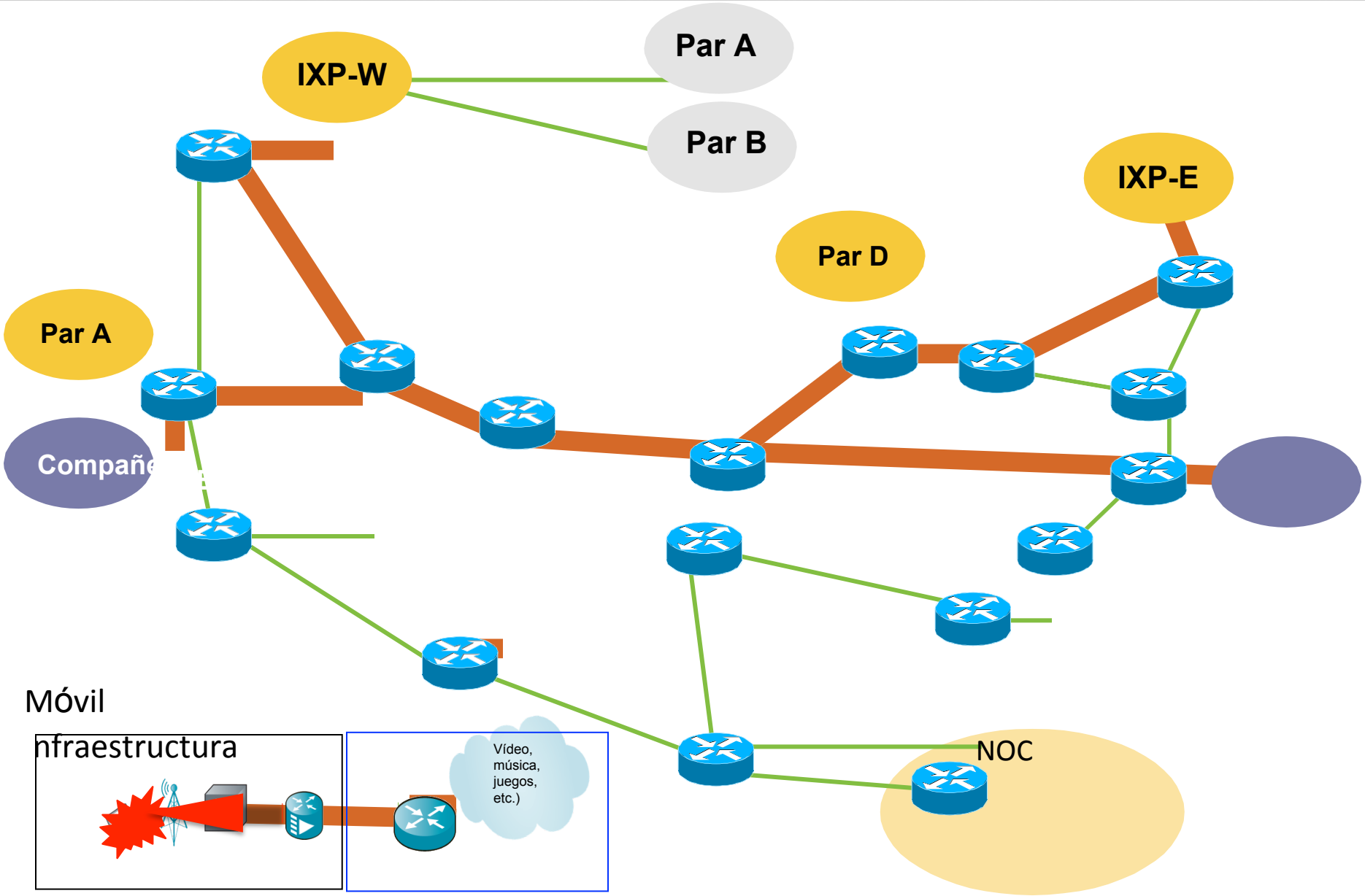
Efectos de un ataque DDoS de reflexión /amplificación de 400 gb/s en la capacidad de la red



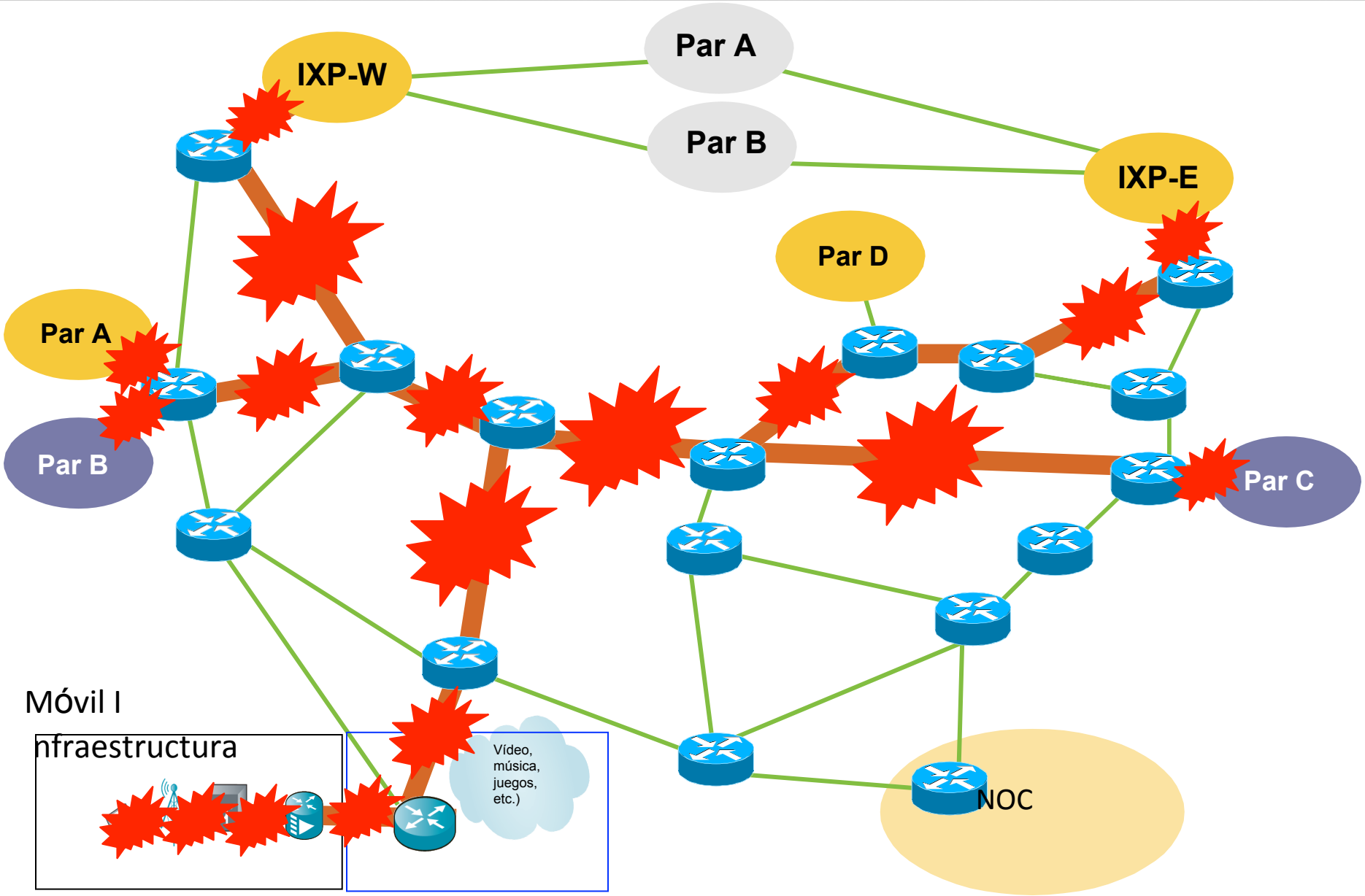
Efectos de un ataque DDoS de reflexión /amplificación de 400 gb/s en la capacidad de la red



Efectos de un ataque DDoS de reflexión /amplificación de 400 gb/s en la capacidad de la red



Efectos de un ataque DDoS de reflexión /amplificación de 400 gb/s en la capacidad de la red



Los dos factores principales que hacen posible estos ataques

- No desplegar ***mecanismos de validación de direcciones de origen (por ejemplo, anti-spoofing)*** como Unicast Reverse-Path Forwarding (uRPF), ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, ACLs, etc. en todos los bordes de las redes de ISP y de empresa.

- ***Servicios mal configurados y abusivos*** que se ejecutan en servidores, routers, switches, dispositivos CPE domésticos, etc.

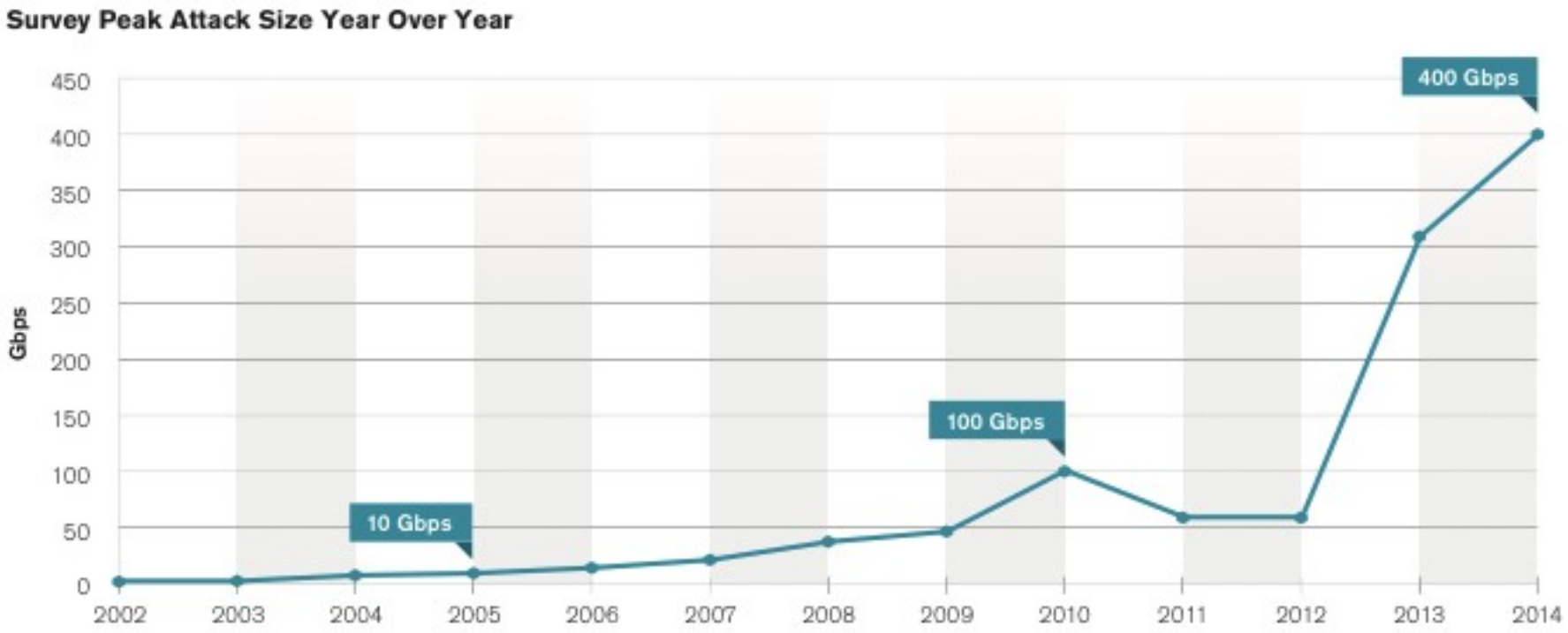
Los dos factores principales que hacen posible estos ataques

- No desplegar ***mecanismos de validación de direcciones de origen (por ejemplo, anti-spoofing)*** como Unicast Reverse-Path Forwarding (uRPF), ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, ACLs, etc. en todos los bordes de las redes de ISP y de empresa.

- ***Servicios mal configurados y abusivos*** que se ejecutan en servidores, routers, switches, dispositivos CPE domésticos, etc.

Crecimiento de los volúmenes de ataques DDoS, 2002 - 2014

Prácticamente *todo el* crecimiento del volumen de ataques DDoS en los últimos 12 años se debe al aumento de la popularidad de las metodologías de reflección/amplificación de ataques DDoS.



La capacidad de falsificar el traffic es *necesaria para* lanzar ataques de reflección/amplificación DDoS.

Factores adicionales que contribuyen

- Los operadores de red no utilizan la ***telemetría de flujos*** (por ejemplo, NetFlow, cflowd/jflow, etc.) para la detección, clasificación y seguimiento de los ataques.
- Los ISP y las empresas no ***escanean de forma proactiva los servicios abusivos*** *en sus redes y no* escanean y alertan a los clientes/usuarios que ejecutan servicios abusivos, ***bloqueando los servicios abusivos*** hasta que sean remediados, si es necesario.
- No desplegar y utilizar eficazmente las ***herramientas de reacción/mitigación de DDoS, como*** Source-Based Remotely-Triggered Blackholing (**S/RTBH**), **flowspec** y Intelligent DDoS Mitigation Systems (**IDMSes**).
- No se ***financia ni se prioriza la disponibilidad por*** igual que la confidencialidad y la integridad en el ámbito de la seguridad.
- Muchas empresas y proveedores de servicios de Internet ***no*** se suscriben a ***"Clean Pipes"***.
  Servicios de mitigación de DDoS ofrecidos por los ISP/MSSP.

¿Qué tipos de dispositivos se utilizan?

- Dispositivos ***de equipos de banda ancha del consumidor (CPE): por*** ejemplo, routers/módems de banda ancha domésticos con configuraciones por defecto inseguras (¡y a veces inseguras!)
- ***Dispositivos de equipos de proveedores (PE) de calidad comercial: por*** ejemplo, ***routers*** más grandes y ***potentes y conmutadores de capa 3*** utilizados por los ISP y las empresas
- ***Servidores (reales o virtuales)*** que ejecutan demonios de servicio mal configurados y abusivos: servidores domésticos instalados por usuarios finales, servidores comerciales instalados por ISP y empresas.
- ***Dispositivos integrados*** como impresoras conectadas a la red (!), DVRs, etc.
- La ***Internet de los objetos se está*** convirtiendo rápidamente en la ***red de bots de los objetos***.

Terminología del ataque de reflexión/amplificación

- ***Origen del ataque***: punto de origen de los paquetes de ataque falsos.
- ***Reflector*** - nodos a través de los cuales los paquetes de ataque falsos son "reflejados" al objetivo del ataque y/o a un nodo amplificador separado antes de ser reflejados al objetivo.
- ***Amplificador*** - nodos que reciben paquetes de ataque no falsificados de los nodos reflectores y luego generan paquetes de respuesta significativamente más grandes, que son enviados de vuelta a los reflectores.
- ***Reflector/Amplificador*** - nodos que realizan tanto la reflexión como la amplificación de los paquetes de ataque, y luego transmiten las respuestas no falsificadas y amplificadas al objetivo final del ataque. Muchos ataques de reflexión/amplificación (no todos) funcionan de esta manera.
- ***Tramo de ataque***: los distintos elementos de la ruta lógica que atraviesa el tráfico de ataque en su camino desde el origen del ataque hasta los reflectores/amplificadores, y desde los reflectores/amplificadores hasta el objetivo del ataque.

Tráfico con spoofing vs. Tráfico sin spoofing

- Origen del ataque - las reflector/amplifier direcciones IP de origen son ***falsificadasEl*** . atacante ***falsifica*** la dirección IP del objetivo final del ataque.
- Si se trata de reflectores y amplificadores separados, el tráfico del reflector al amplificador ***no se falsifica***, el tráfico del amplificador de vuelta al reflector ***no se falsifica***, y el tráfico del reflector al objetivo del ataque ***no se falsifica***.
- Si se trata de reflectores/amplificadores combinados, el tráfico desde los reflectores/amplificadores hacia el objetivo del ataque ***no*** se ***falsifica***.
- Esto significa que el objetivo del ataque ve las ***direcciones IP reales*** del tráfico de ataque que lo azota en el último tramo del ataque.
- Este hecho tiene importantes ***implicaciones positivas para las opciones de mitigación*** disponibles para el objetivo del ataque, pero ***el gran número de IPs de origen*** es a menudo un factor de complicación.

Cinco vectores comunes de reflexión/amplificación

- **chargen** – 30-year-old tool for testing network link integrity and performance. Rara vez (¿alguna vez?) se utiliza hoy en día para su propósito – 30-year-old tool for testing network link integrity and performance. original. Implantado de forma absurda y sin sentido en la era moderna por vendedores de dispositivos empotrados que no tienen ni idea.
- **DNS**: el Sistema de Nombres de Dominio resuelve los nombres de uso humano en direcciones IP. Forma parte del "plano de control" de Internet. Sin DNS no hay Internet.
- **SNMP** - Simple Network Management Protocol. Se utiliza para supervisar y, opcionalmente, configurar dispositivos de infraestructura de red, servicios, etc.
- **NTP** - Network Time Protocol proporciona servicios de sincronización de tiempo para su routers/switches/laptops/tablets/phones/etc. El servicio de Internet más importante del que nunca ha oído hablar.
- **SSDP** - Simple Services Discovery Protocol actúa como un sistema de enumeración de servicios mal diseñado e implementado para el UPnP mal diseñado e implementado.

La reflexión/amplificación no se limita a estos cinco vectores

- Muchos protocolos/servicios pueden ser aprovechados por los atacantes para lanzar ataques DDoS de reflexión/amplificación.
- Estos cinco - DNS, chargen, SNMP, SSDP y NTP - son vectores de reflexión/amplificación comúnmente observados.
- La mayoría de los ataques de reflexión/amplificación (no todos) utilizan UDP.
- Los mismos principios generales expuestos en relación con estos cinco vectores se aplican también a otros.
- Hay diferencias específicas de protocolo/servicio que también se aplican.
- Los atacantes están investigando y utilizando activamente otros vectores de reflexión/amplificación, también - ¡esté preparado!

Cinco vectores comunes de reflexión/amplificación

Abreviatura	Protocolo	Puertos	Factor de Ampliación	# Servidores Abusables
CHARGEN	Protocolo de generación de personajes	UDP / 19	18x/1000x	Decenas de miles (90K)
DNS	Sistema de nombres de dominio	UDP / 53	160x	Millones (27M)
NTP	Protocolo de tiempo de red	UDP / 123	1000x	Más de cien mil (119K)
SNMP	Protocolo simple de gestión de redes	UDP / 161	880x	Millones (5M)
SSDP	Protocolo simple de descubrimiento de servicios	UDP /1900	20x/83x	Millones (2M)

Reflección/Amplificación NTP

Factor de amplificación - NTP

Abreviatura	Protocolo	Puertos	Factor de Ampliación	# Servidores Abusables
CHARGEN	Protocolo de generación de personajes	UDP / 19	18x/1000x	Decenas de miles (90K)
DNS	Sistema de nombres de dominio	UDP / 53	160x	Millones (27M)
NTP	Protocolo de tiempo de red	UDP / 123	1000x	Más de cien mil (119K)
SNMP	Protocolo simple de gestión de redes	UDP / 161	880x	Millones (5M)
SSDP	Protocolo simple de descubrimiento de servicios	UDP /1900	20x/83x	Millones (2M)

Características de un ataque de reflexión/amplificación

- El atacante ***falsifica*** la dirección IP del objetivo del ataque, envía *monlist*, *showpeers* u otras consultas administrativas de nivel 6/-7 de NTP a múltiples servicios NTP abusables que se ejecutan en servidores, routers, dispositivos CPE domésticos, etc.
- El atacante elige el puerto UDP al que quiere dirigirse - normalmente, UDP/80 o UDP/123, pero puede ser ***cualquier puerto a elección del*** atacante- y lo utiliza como origen port. El ***puerto de destino es UDP/123***.
- Los servicios NTP "responden" al objetivo del ataque con flujos ***no suplantados*** de paquetes de ~468 bytes ***procedentes de UDP/123*** hacia el objetivo***; el puerto de destino es el puerto de origen que el atacante eligió*** al generar las consultas NTP *monlist/showpeers/etc.*

Características de un ataque de reflexión/amplificación (cont.)

- A medida que convergen estos múltiples flujos de respuestas NTP ***no falsificadas***, el volumen de los ataques puede ser ***enorme***: el mayor ataque verificado de este tipo hasta ahora es de ***más de 300gb/seg***. Los ataques de ***100gb/seg*** son habituales.
- Debido al gran volumen de los ataques, el ancho de ***banda de tránsito de Internet*** del objetivo, junto con el ancho de banda central de los pares/subidas del objetivo, así como el ancho de banda central de las redes intermediarias entre los diversos servicios NTP de los que se está abusando y el objetivo, se ***satura*** con tráfico de ataque ***no falsificado***.
- En la mayoría de los ataques, los atacantes aprovechan entre ~4.000 y ~7.000 servicios NTP abusables. En algunos ataques se han observado ***hasta 50.000 servicios NTP***.

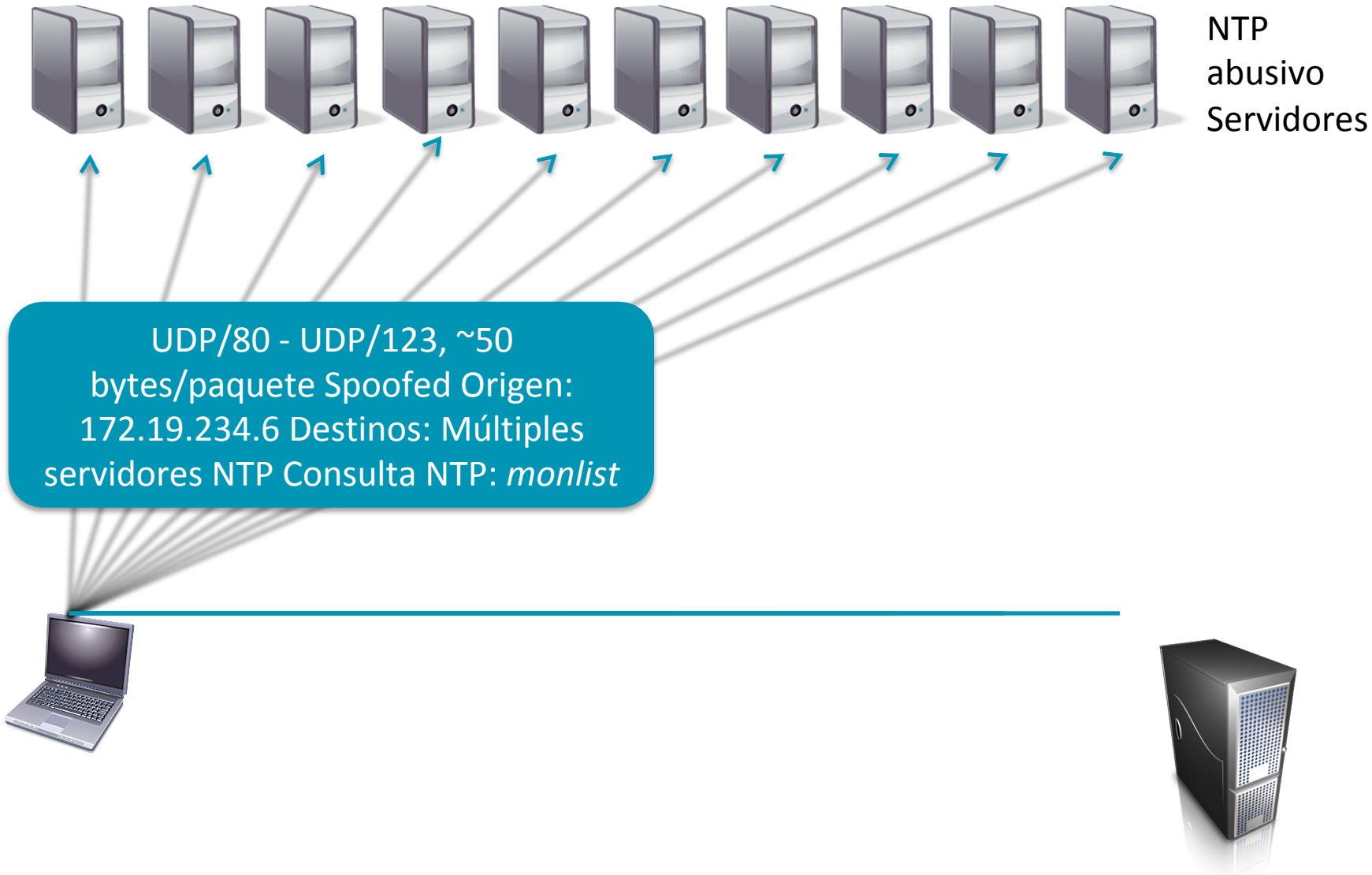
Metodología de ataque de reflexión/amplificación

NTP abusivo Servidores

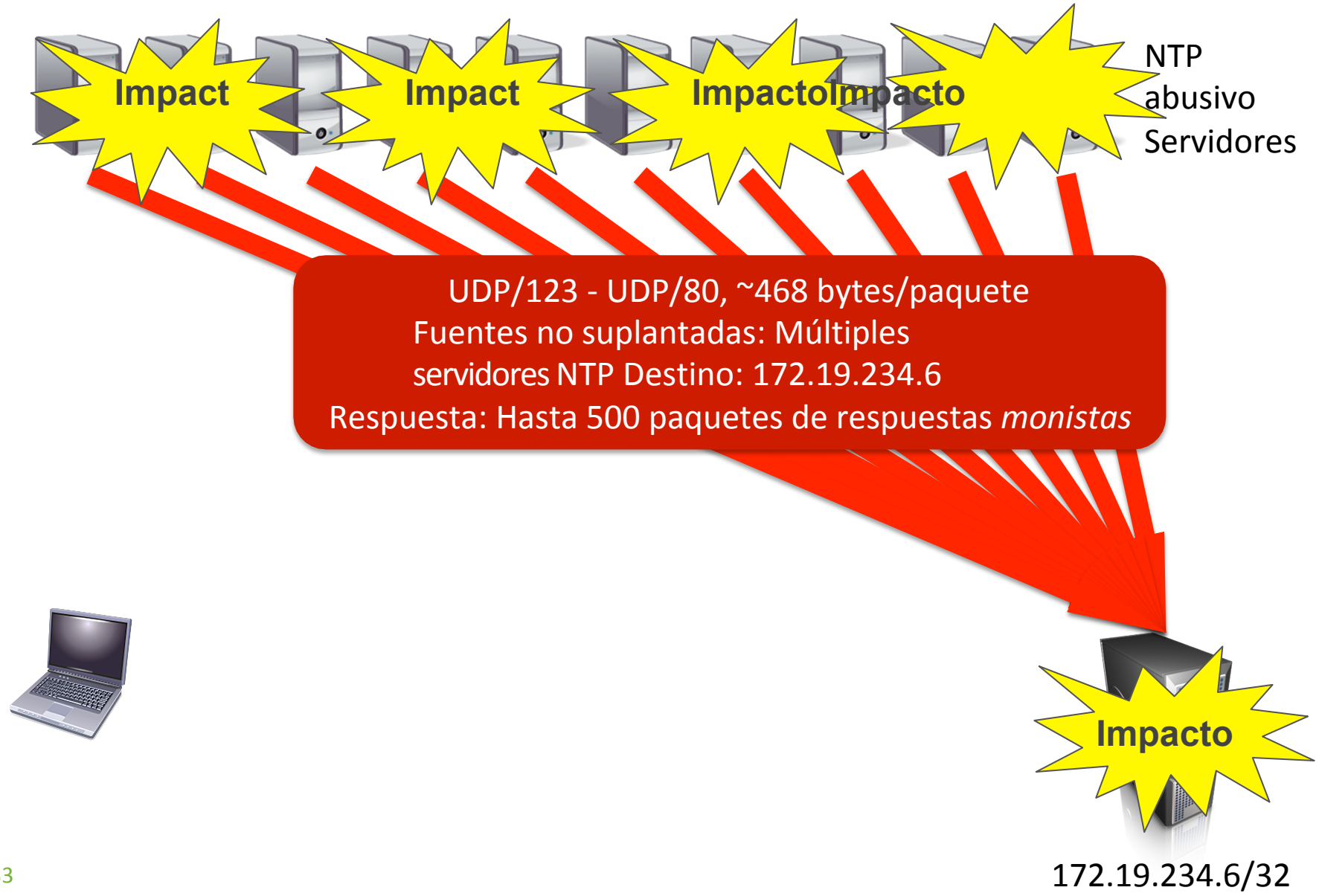
Internet--Servidores accesibles, routers, dispositivos CPE domésticos,

172.19.234.6/32

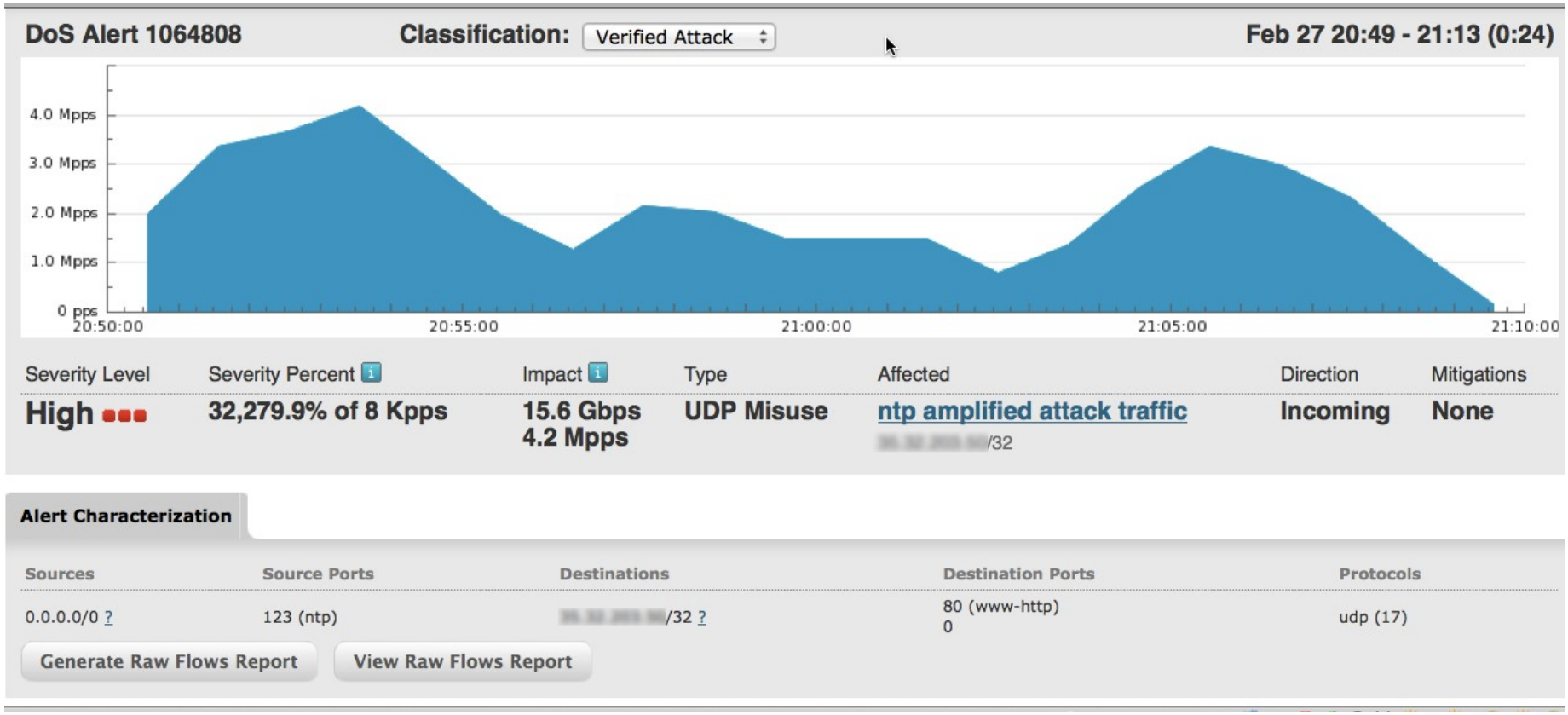
Metodología de ataque de reflexión/amplificación



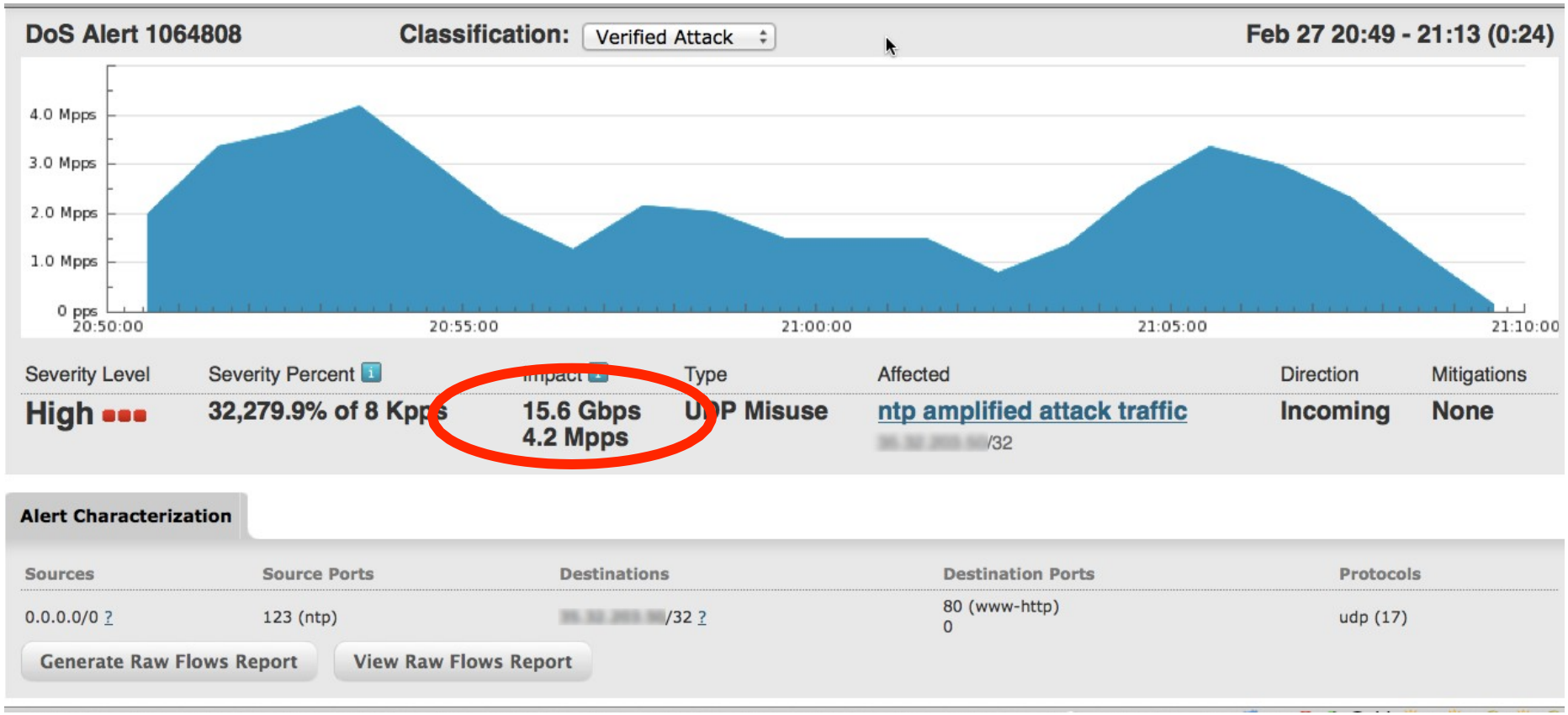
Metodología de ataque de reflexión/amplificación



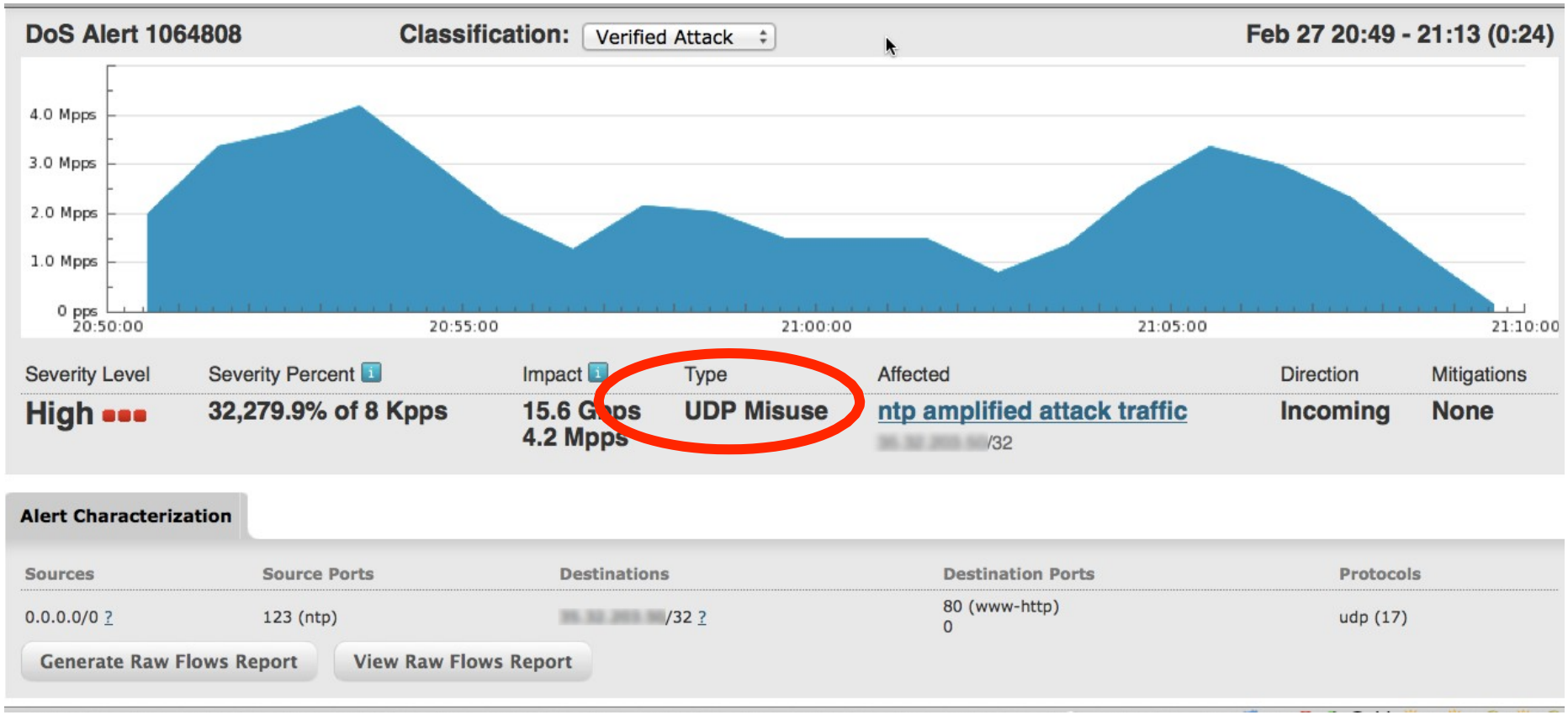
Ataque de reflexión/amplificación NTP



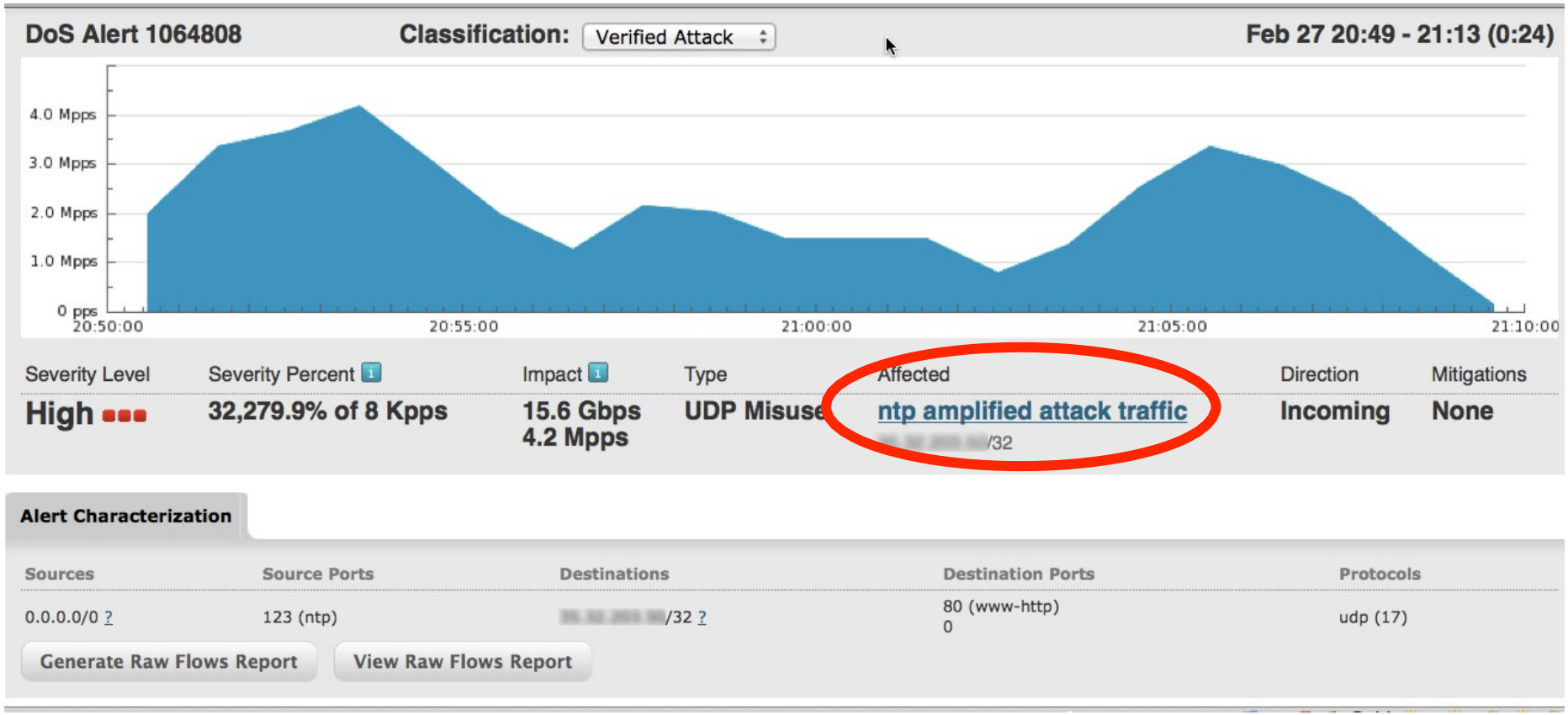
Ataque de reflexión/amplificación NTP



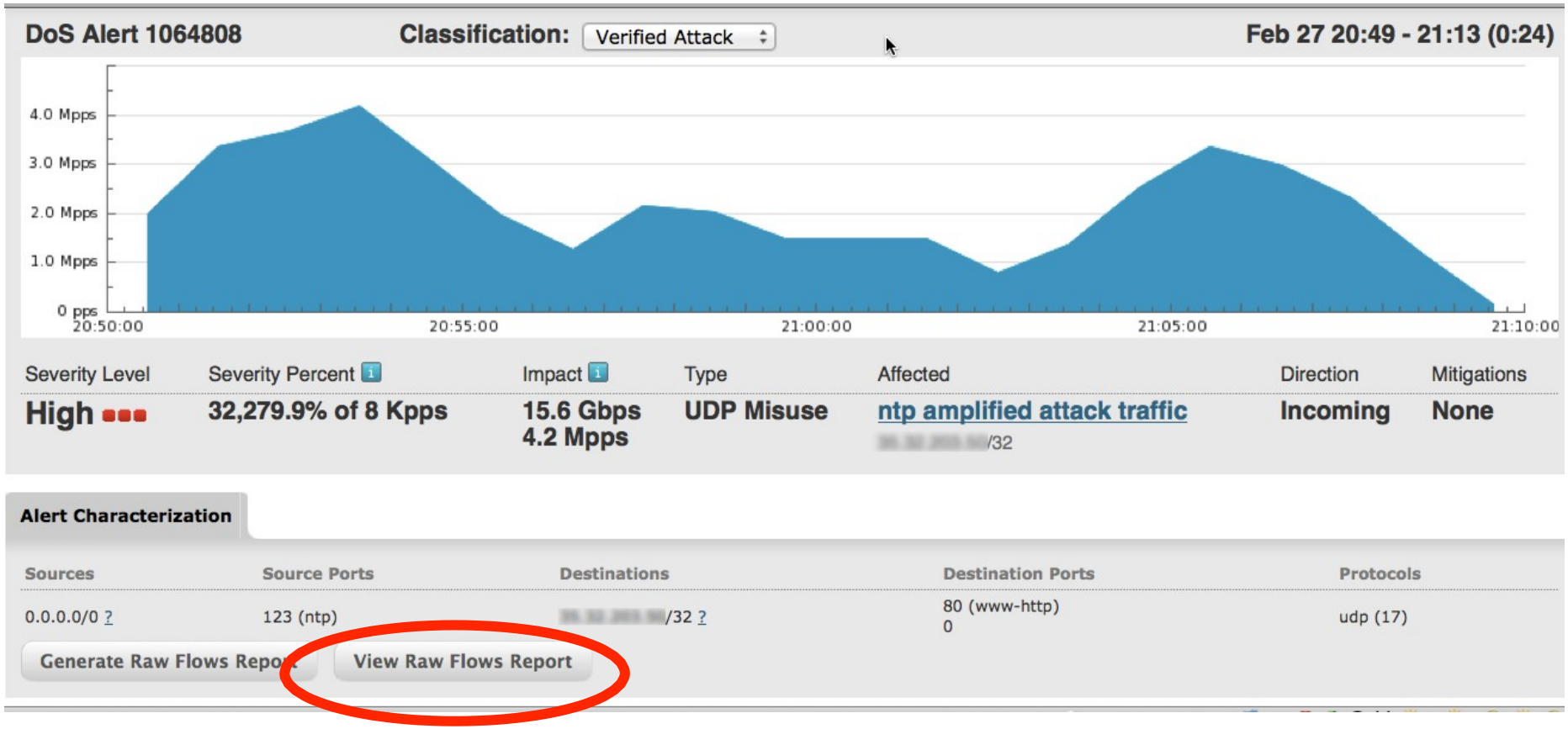
Ataque de reflexión/amplificación NTP



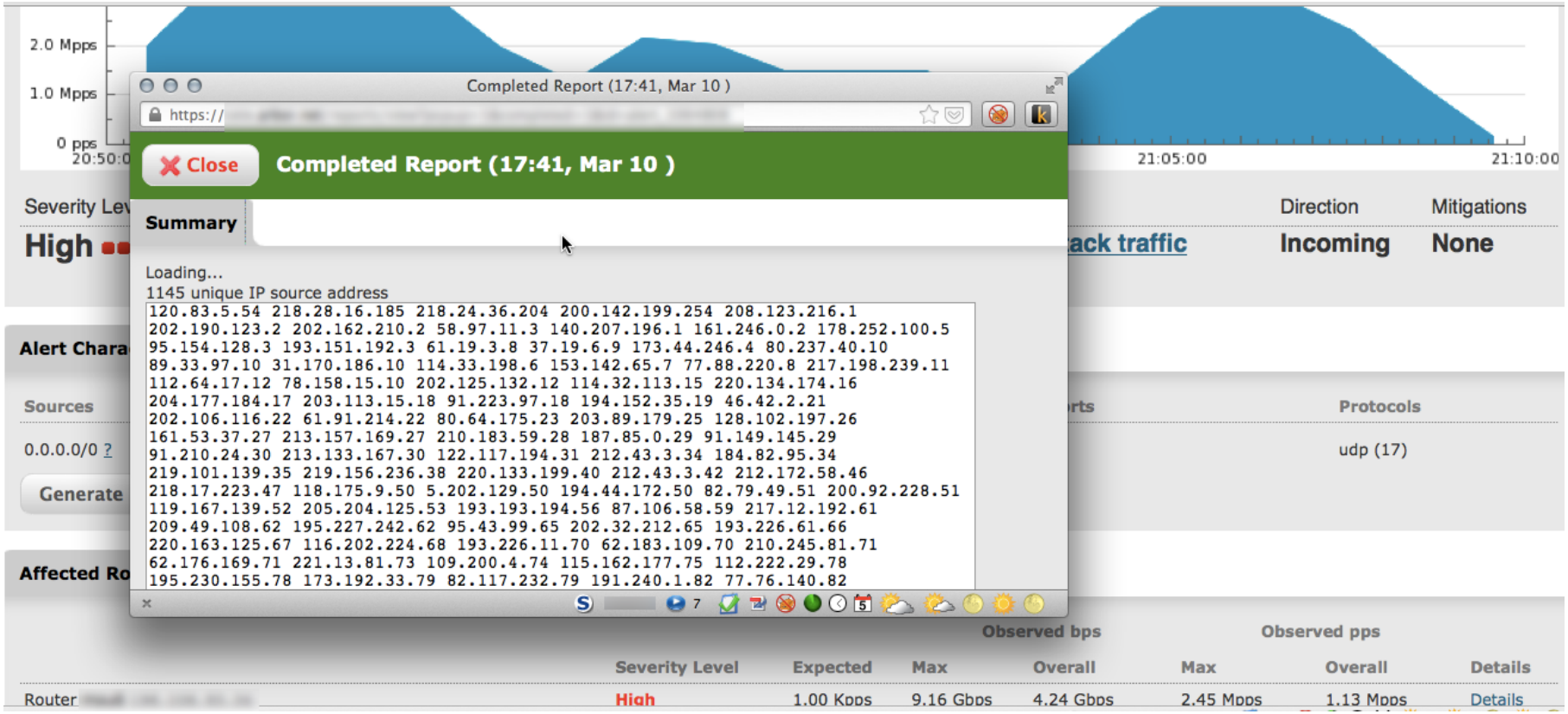
Ataque de reflexión/amplificación NTP



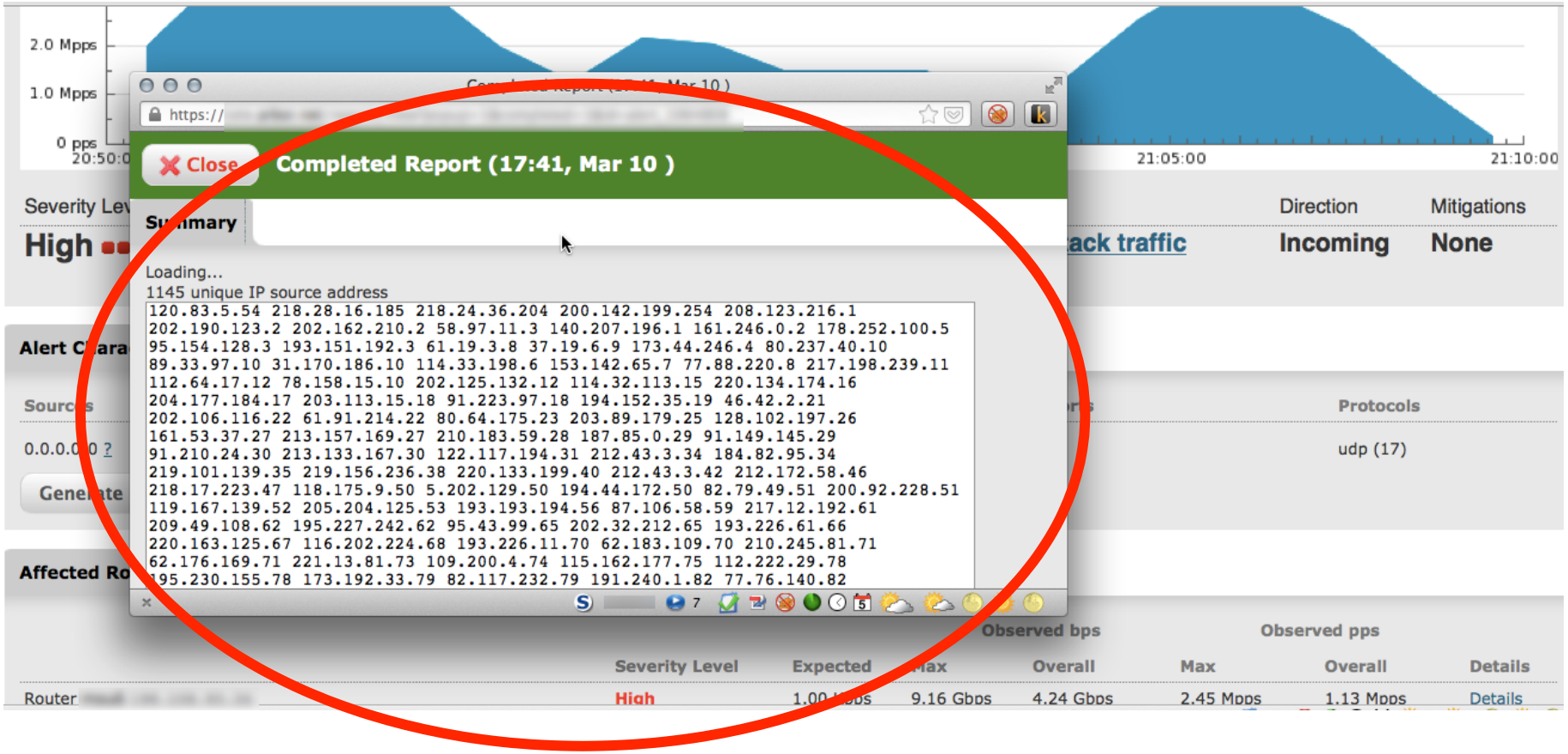
Ataque de reflexión/amplificación NTP



Ataque de reflexión/amplificación NTP



Ataque de reflexión/amplificación NTP



Ataque de reflexión/amplificación NTP

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	1.00 Kpps	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Interface (SNMP 120) xe-0/0/0.22 [redacted]		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router [redacted]	High	1.00 Kpps	5.52 Gbps	2.60 Gbps	1.48 Mpps	695.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	2.17 Gbps	1.12 Gbps	580.42 Kpps	298.98 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

Ataque de reflexión/amplificación NTP

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	1.00 Kpps	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Interface (SNMP 120) xe-0/0/0.22 [redacted]		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router [redacted]	High	1.00 Kpps	5.52 Gbps	2.60 Gbps	1.48 Mpps	695.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	2.17 Gbps	1.12 Gbps	580.42 Kpps	298.98 Kpps	Details

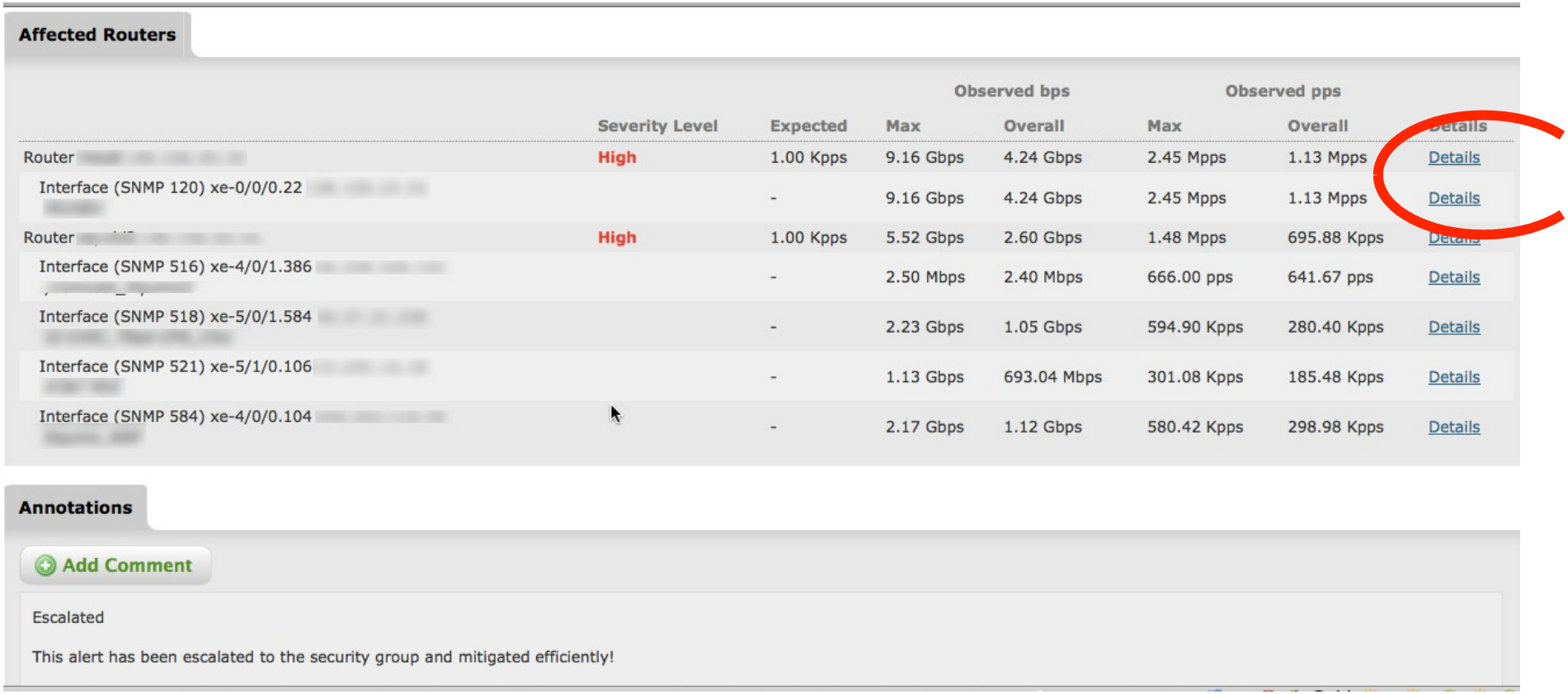
Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

Ataque de reflexión/amplificación NTP



Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	1.00 Kpps	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Interface (SNMP 120) xe-0/0/0.22 [redacted]		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router [redacted]	High	1.00 Kpps	5.52 Gbps	2.60 Gbps	1.48 Mpps	695.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	2.17 Gbps	1.12 Gbps	580.42 Kpps	298.98 Kpps	Details

Annotations

Add Comment

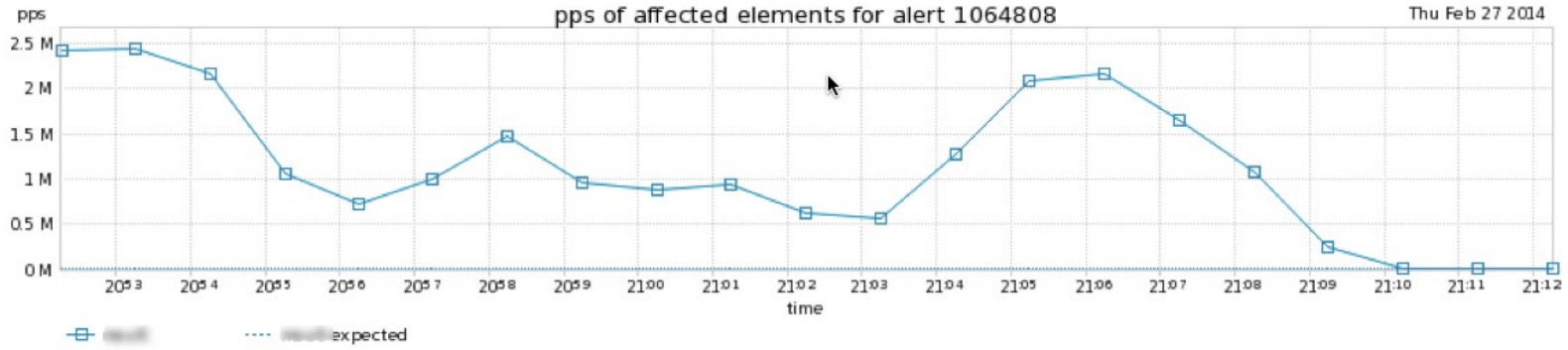
Escalated

This alert has been escalated to the security group and mitigated efficiently!

Ataque de reflexión/amplificación NTP

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1064808	High 32,279.9% Of 8.0 Kpps	15.61 Gbps 4.17 Mpps	0:24 (Ended)	Thu, Feb 27 2014, 20:49:34	Incoming	UDP (Misuse)	ntp amplified attack traffic [redacted]/32 ntp amplified attack traffic



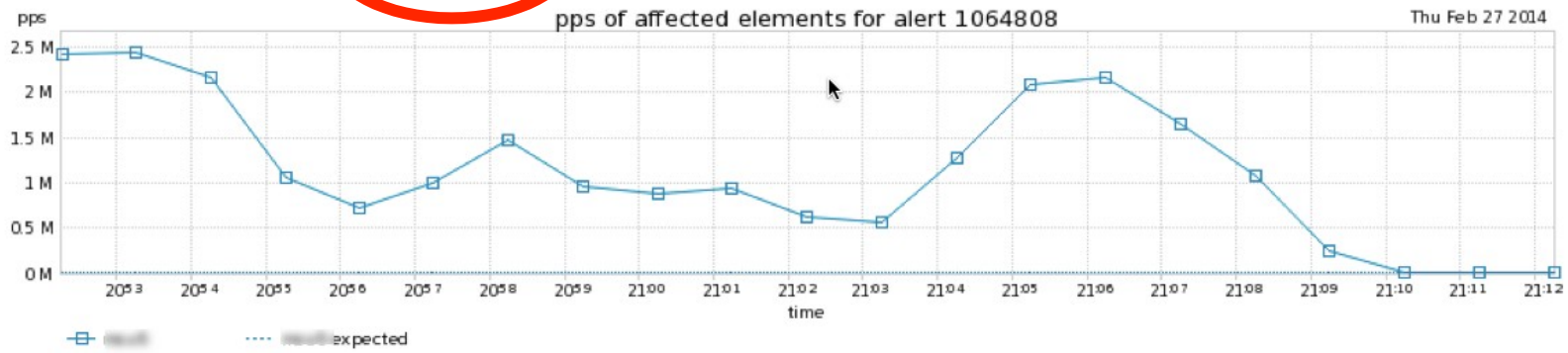
Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	1.00 kpps	9.16 G	4.24 G	2.45 M	1.13 M

Ataque de reflexión/amplificación NTP

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1064808	High 32,279.9% Of 8.0 Kpps	15.61 Gbps 4.17 Mpps	0:24 (Ended)	Thu, Feb 27 2014, 20:49:34	Incoming	UDP (Misuse)	ntp amplified attack traffic [redacted]/32 ntp amplified attack traffic



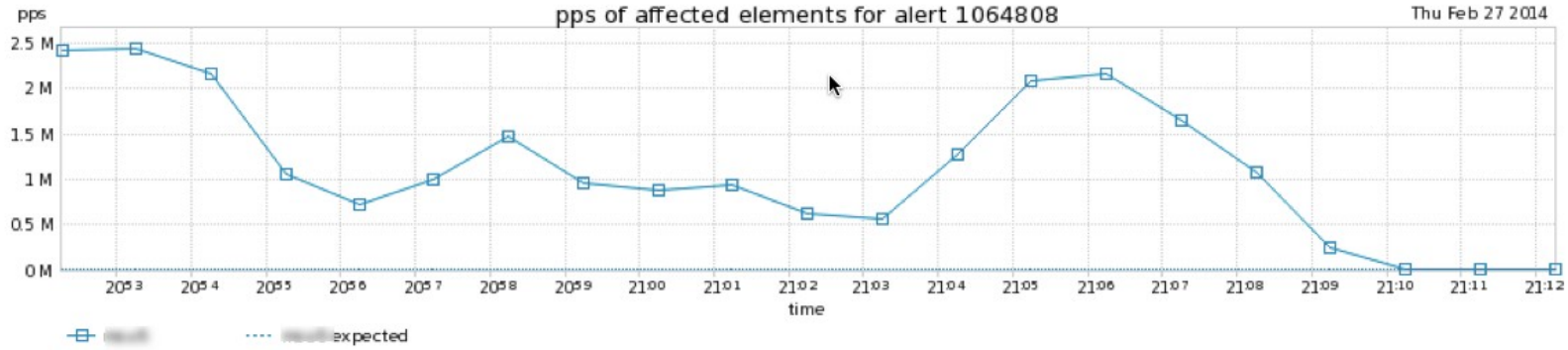
Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	1.00 kpps	9.16 G	4.24 G	2.45 M	1.13 M

Ataque de reflexión/amplificación NTP

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1064808	High 32,279.9% Of 8.0 Kpps	15.61 Gbps 4.17 Mpps	0:24 (Ended)	Thu, Feb 27 2014, 20:49:34	Incoming	UDP (Misuse)	ntp amplified attack traffic [redacted]/32 ntp amplified attack traffic



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	1.00 kpps	9.16 G	4.24 G	2.45 M	1.13 M

Ataque de reflexión/amplificación NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Ataque de reflexión/amplificación NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Ataque de reflexión/amplificación NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Ataque de reflexión/amplificación NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Ataque de reflexión/amplificación NTP

http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.22	120	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.32	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20	157	113.86 G	243.38 M	467.82	723.49 M	193.31 k	17.06	☑

For assistance with this product, please contact support@arbornetworks.com. About

Ataque de reflexión/amplificación NTP

http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.22 [redacted]	120	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.32 [redacted]	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20 [redacted]	157	113.86 G	243.38 M	467.82	723.49 M	193.31 k	17.06	☑

For assistance with this product, please contact support@arbornetworks.com. About

Ataque de reflexión/amplificación NTP

http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.22	120	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.32	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20	157	113.86 G	243.38 M	467.82	723.49 M	193.31 k	17.06	☑

For assistance with this product, please contact support@arbornetworks.com. About

Reflección/Amplificación del DNS

Factor de amplificación - DNS

Abreviatura	Protocolo	Puertos	Factor de Ampliación	# Servidores Abusables
CHARGEN	Protocolo de generación de personajes	UDP / 19	18x/1000x	Decenas de miles (90K)
DNS	Sistema de nombres de dominio	UDP / 53	160x	Millones (27M)
NTP	Protocolo de tiempo de red	UDP / 123	1000x	Más de cien mil (119K)
SNMP	Protocolo simple de gestión de redes	UDP / 161	880x	Millones (5M)
SSDP	Protocolo simple de descubrimiento de servicios	UDP /1900	20x/83x	Millones (2M)

Características de un ataque de reflexión/amplificación

- El atacante falsifica la dirección IP del objetivo del ataque, enviando consultas DNS para registros DNS de gran tamaño previamente identificados (registros ANY, registros TXT de gran tamaño, etc.), bien a servidores DNS recursivos abiertos que puedan ser objeto de abuso, o bien directamente a servidores DNS autoritativos.
- El atacante elige el puerto UDP al que quiere dirigirse - con DNS, esto se limita normalmente a UDP/53 o UDP/1024-65535El puerto de destino es UDP/53
- Los servidores "responden" directamente al objetivo del ataque o al servidor intermedio recursivo DNS abierto con grandes respuestas DNS - el objetivo del ataque verá flujos de respuestas DNS no solicitadas desglosadas en fragmentos iniciales y no iniciales.
- El tamaño de las respuestas suele ser de 4096 - 8192 bytes (puede ser menor o mayor), dividido en múltiples fragmentos.
- El tamaño de los paquetes que recibe el objetivo del ataque suele ser de ~1500 bytes debido a las MTU de Ethernet predominantes, y son muchas.

Características de un ataque de reflexión/amplificación (cont.)

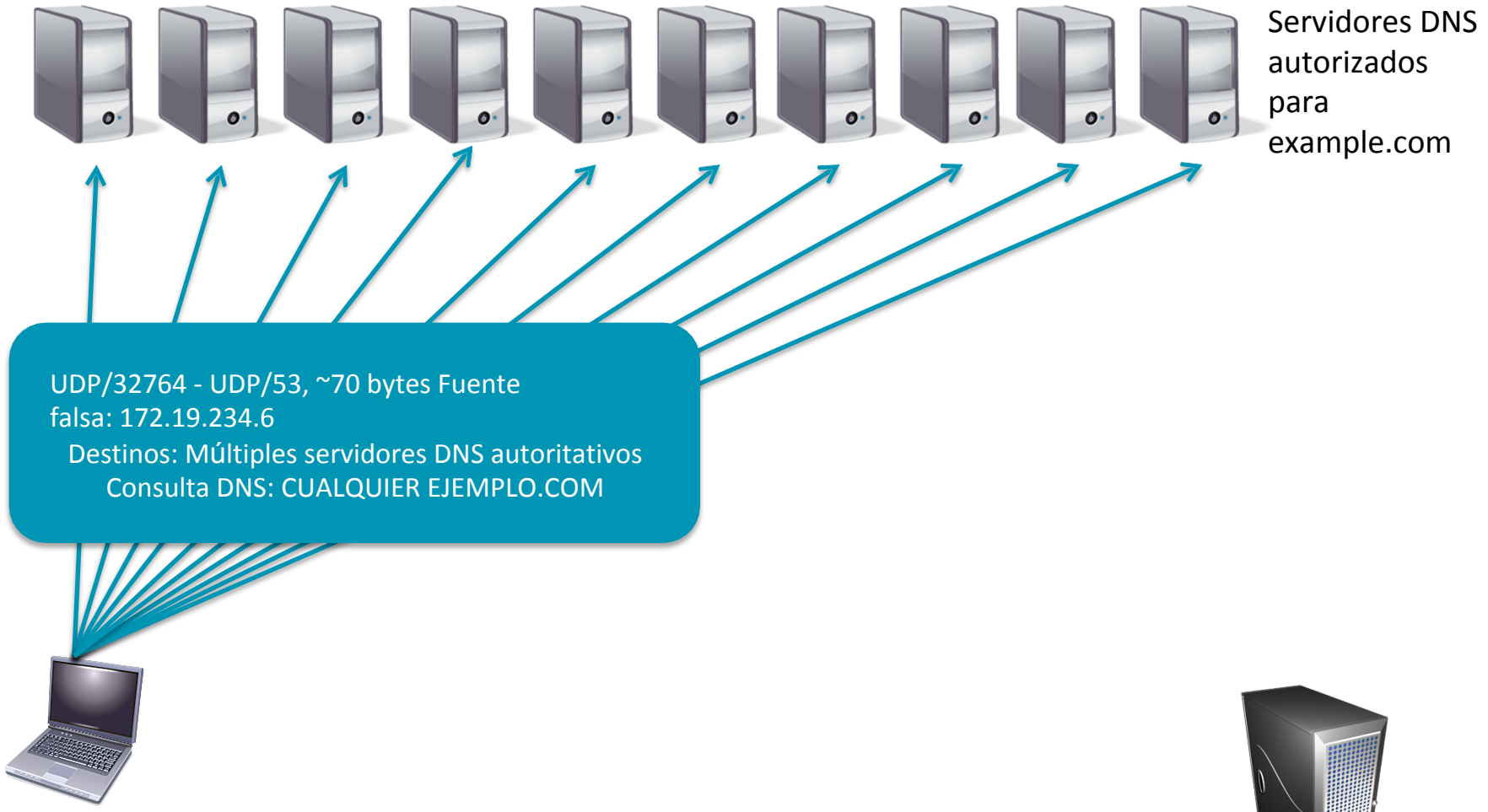
- A medida que convergen estos múltiples flujos de respuestas DNS fragmentadas, el volumen de los ataques puede ser enorme: el mayor ataque verificado de este tipo hasta ahora es de ~200gb/sec. 100gb/seg.
- El ancho de banda de tránsito de Internet del objetivo, junto con el ancho de banda central de los pares/sobrecarga del objetivo, así como el ancho de banda central de las redes intermediarias entre los distintos servicios DNS de los que se abusa y el objetivo, están saturados.
- En la mayoría de los ataques que implican servidores DNS recursivos abiertos intermedios son reflectores, entre ~20.000 - 30.000 DNS recursivos abusables son aprovechados por los atacantes. En algunos ataques se han observado hasta 50.000 servidores DNS recursivos abiertos abusables.
- En los ataques que aprovechan directamente los servidores DNS autorizados, los atacantes utilizan cientos o miles de estos servidores.
- Muchos de los servidores DNS autoritativos más conocidos son anycasted, con múltiples instancias desplegadas en Internet.

Metodología de ataque de reflexión/amplificación de DNS #1

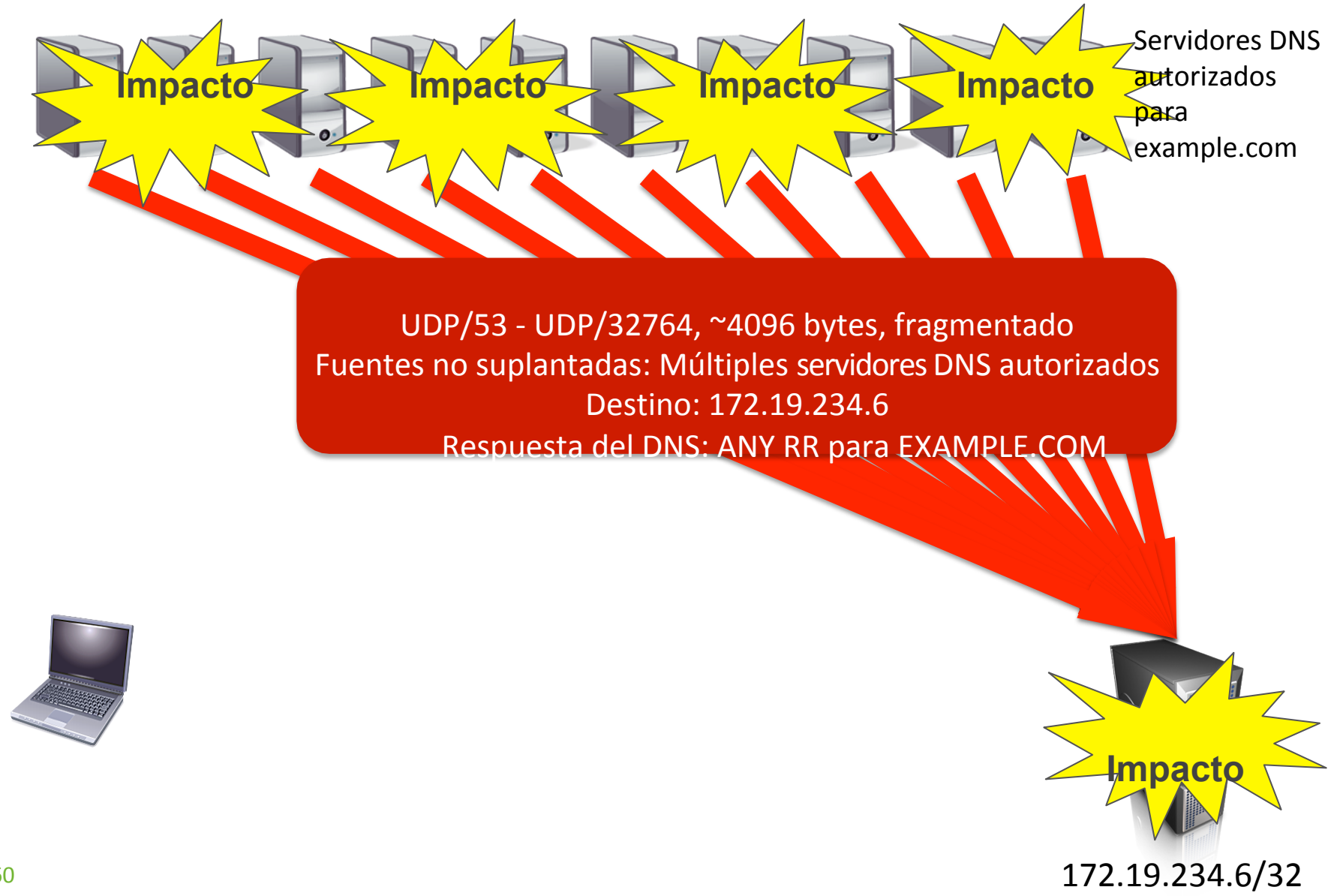
Servidores DNS autorizados para example.com

172.19.234.6/32

Metodología de ataque de reflexión/amplificación de DNS #1



Metodología de ataque de reflexión/amplificación de DNS #1



Metodología de ataque de reflexión/amplificación de DNS #2

Servidores DNS autorizados para example.com

DNS Recursivo Abusable Servidores

172.19.234.6/32

Metodología de ataque de reflexión/amplificación de DNS #2

172.19.234.6/32

Metodología de ataque de reflexión/amplificación de DNS #2

172.19.234.6/32

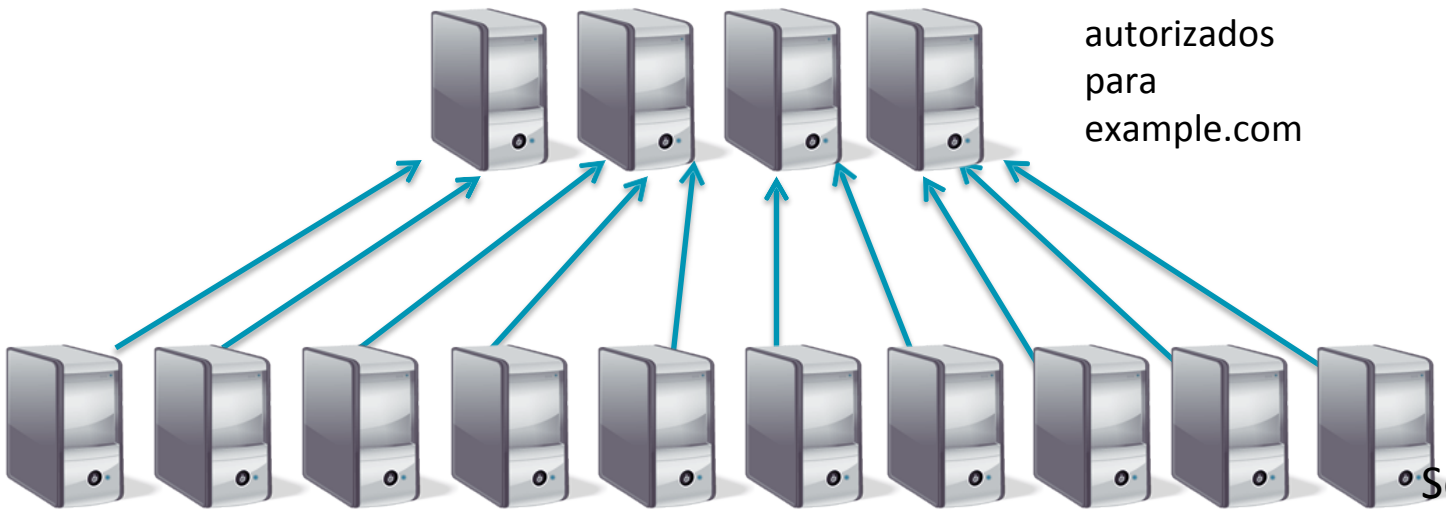
Metodología de ataque de reflexión/amplificación de DNS #2

Servidores DNS autorizados para example.com

DNS Recursivo Abusable Servidores

172.19.234.6/32

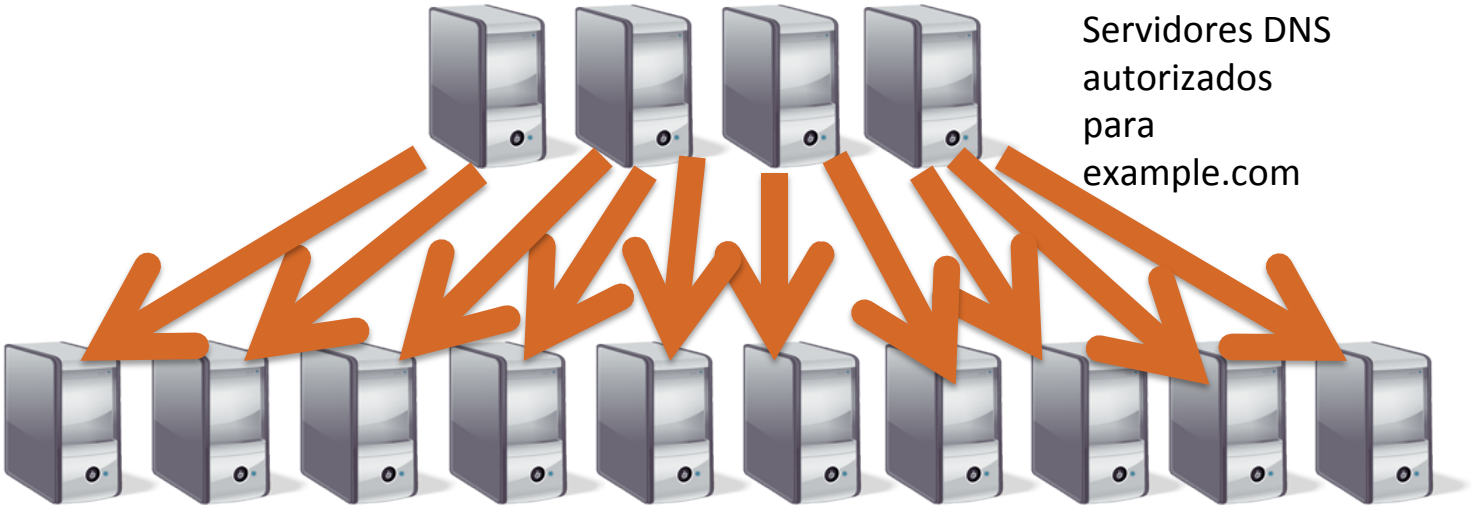
Metodología de ataque de reflexión/amplificación de DNS #2



UDP/vario- UDP/53, ~70 bytes
Fuentes no suplantadas: Múltiples servidores DNS recursivos Destinos: Múltiples servidores DNS autoritativos
Consulta DNS: TXT PGP.EJEMPLO.COM

172.19.234.6/32

Metodología de ataque de reflexión/amplificación de DNS #2



172.19.234.6/32

Metodología de ataque de reflexión/amplificación de DNS #2

172.19.234.6/32

Metodología de ataque de reflexión/amplificación de DNS #2

172.19.234.6/32

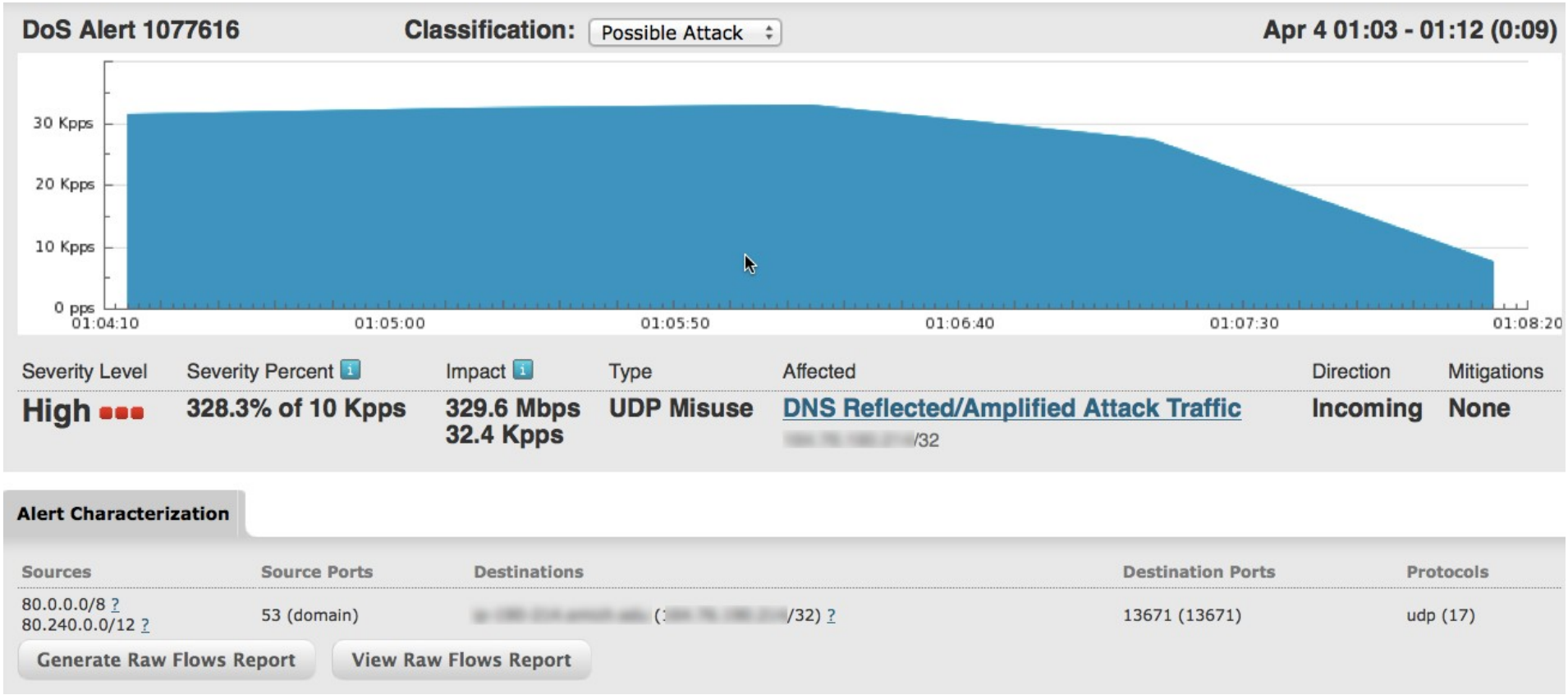
Metodología de ataque de reflexión/amplificación de DNS #2

172.19.234.6/32

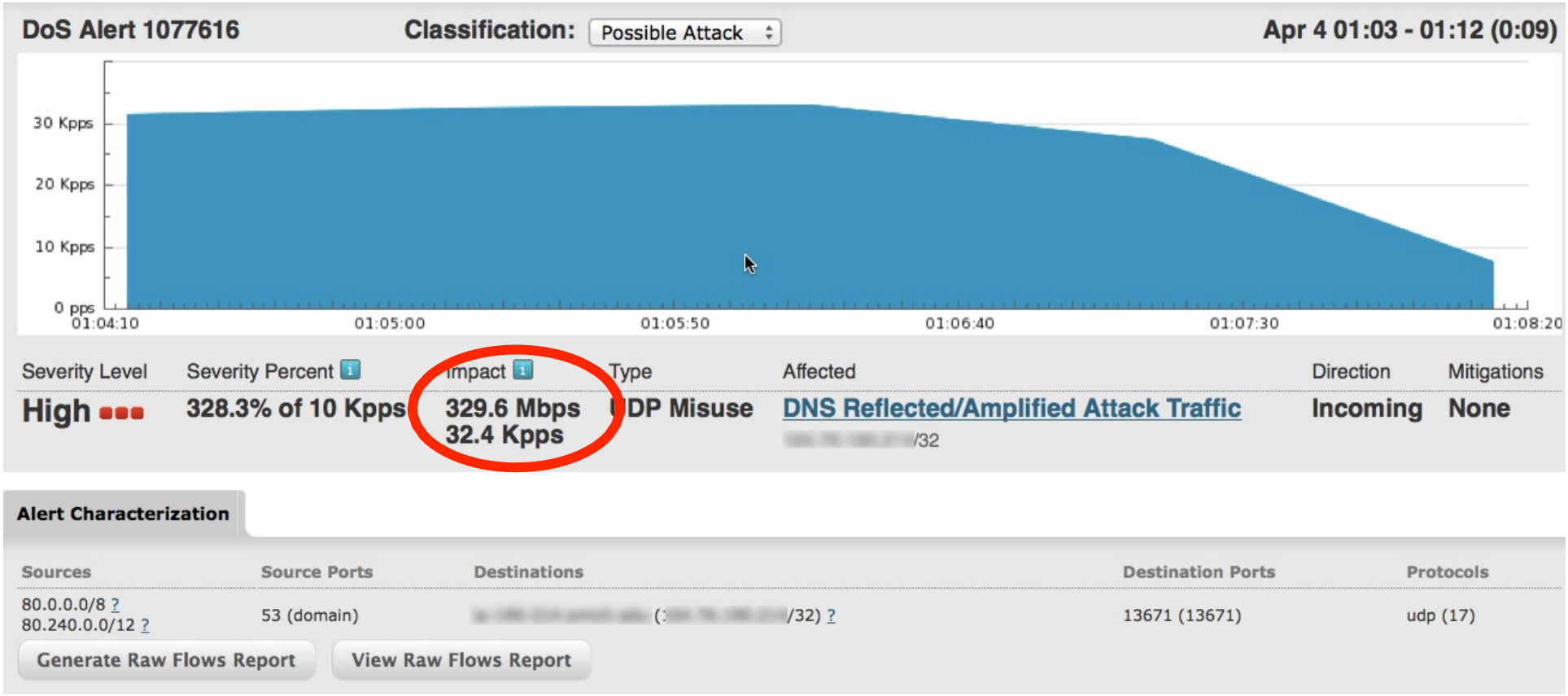
Metodología de ataque de reflexión/amplificación de DNS #2

172.19.234.6/32

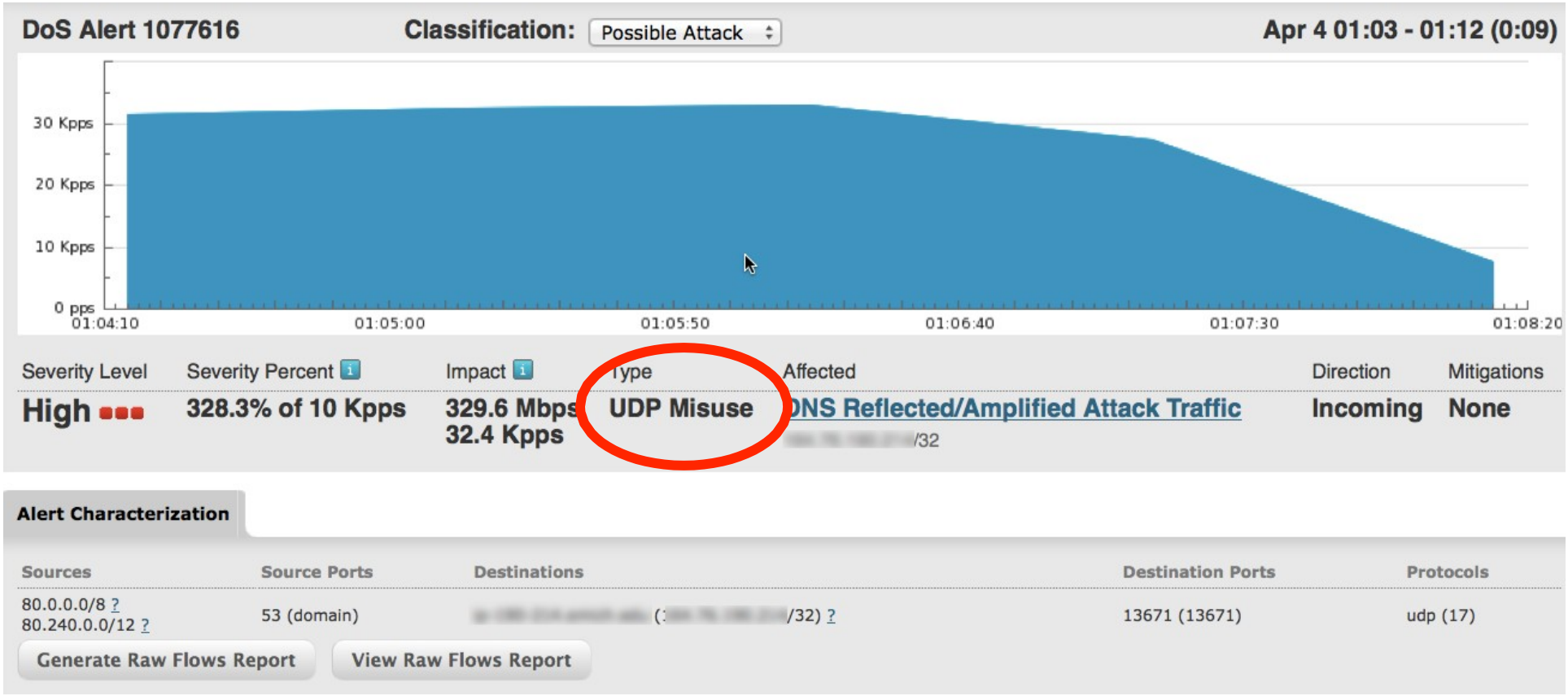
Ataque de reflexión/amplificación de DNS - UDP/53



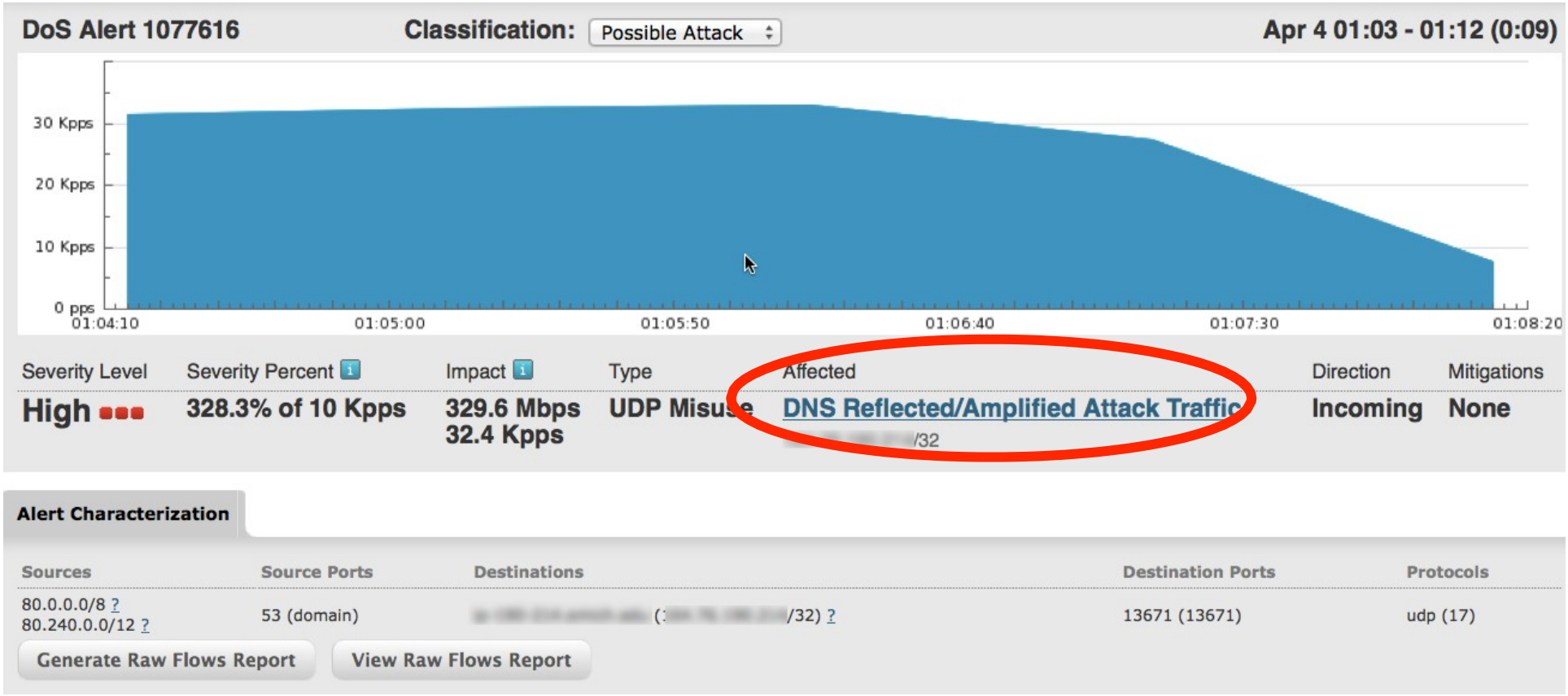
Ataque de reflexión/amplificación de DNS - UDP/53



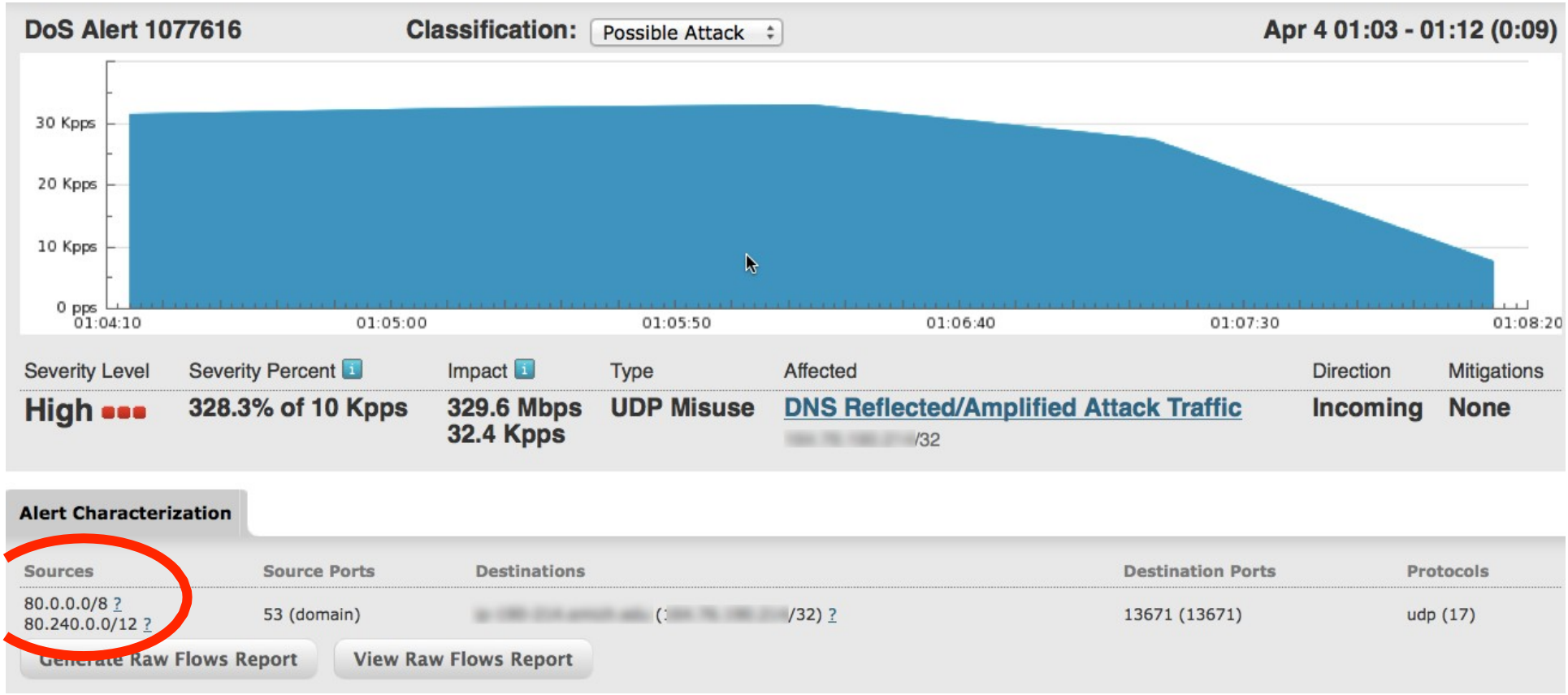
Ataque de reflexión/amplificación de DNS - UDP/53



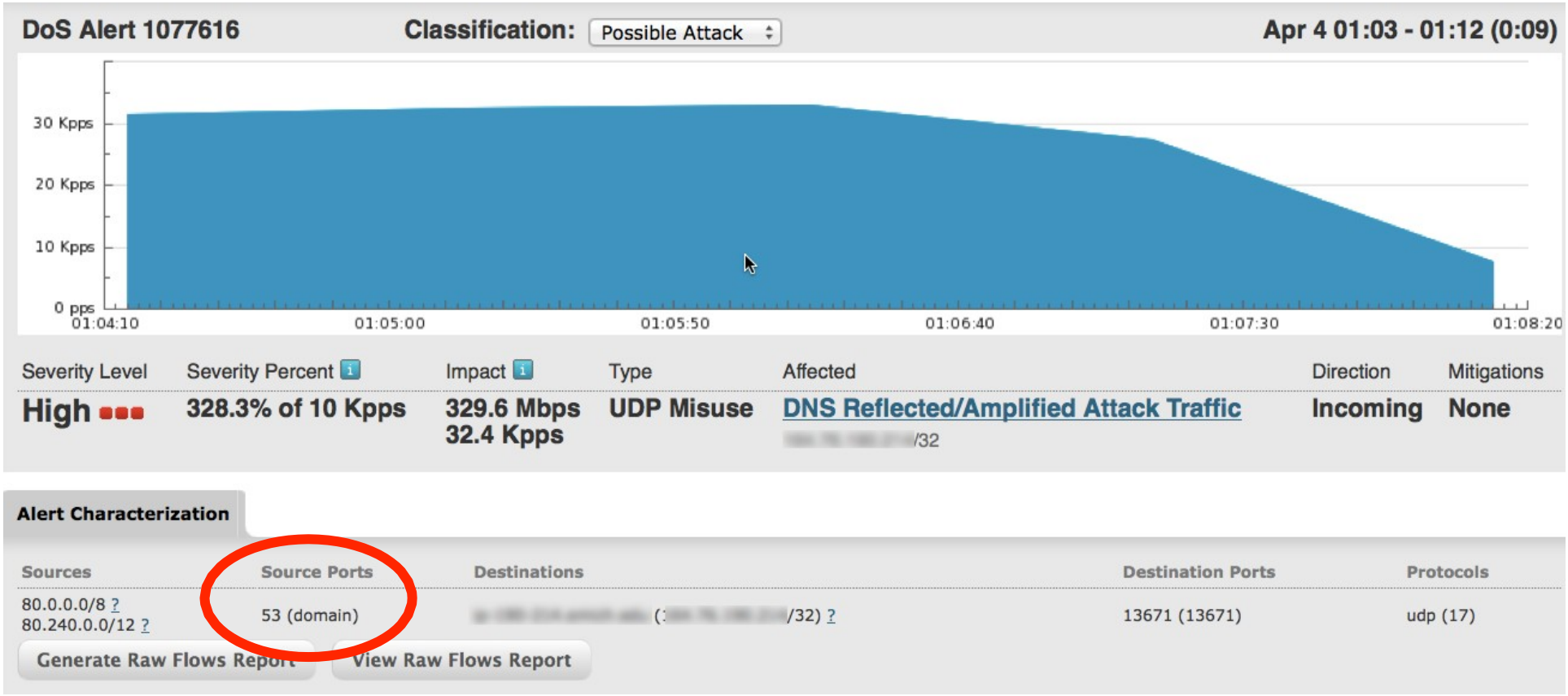
Ataque de reflexión/amplificación de DNS - UDP/53



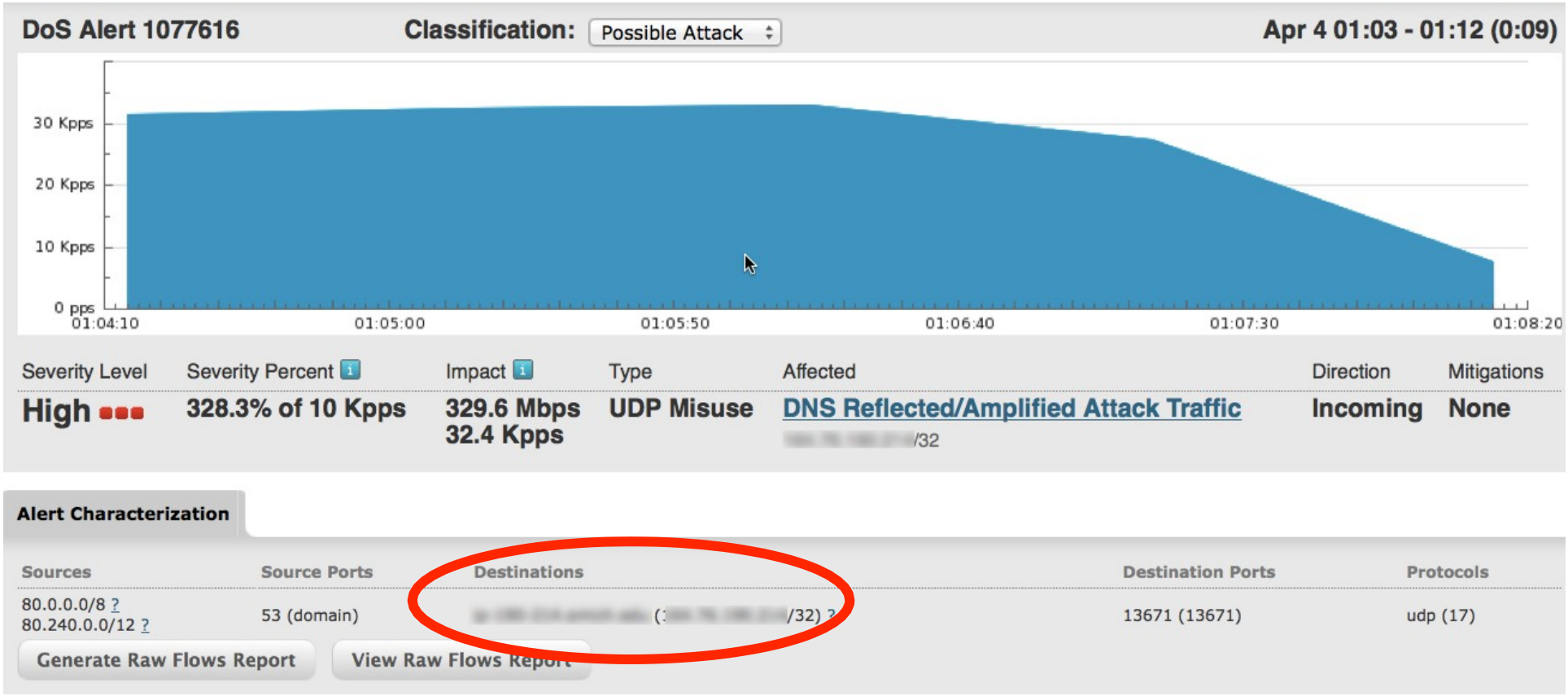
Ataque de reflexión/amplificación de DNS - UDP/53



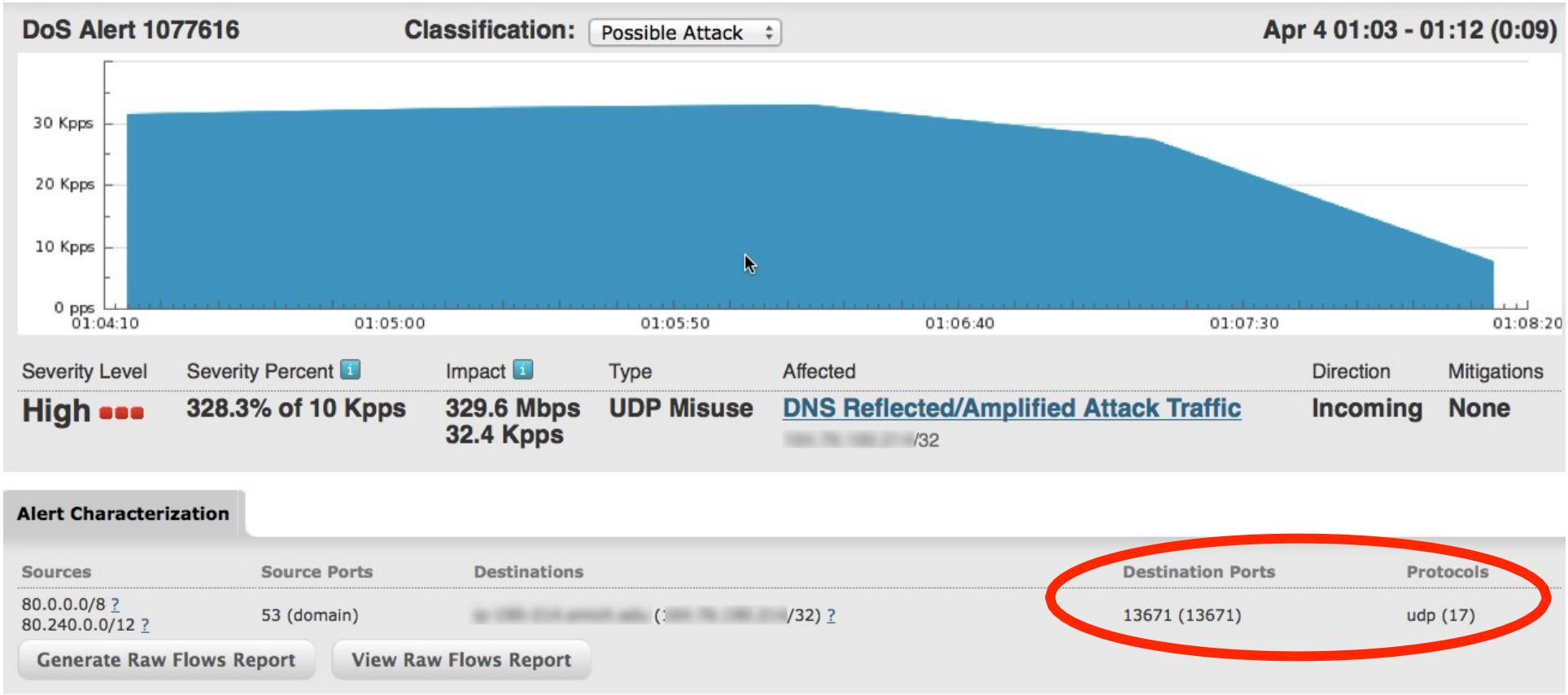
Ataque de reflexión/amplificación de DNS - UDP/53



Ataque de reflexión/amplificación de DNS - UDP/53



Ataque de reflexión/amplificación de DNS - UDP/53



Ataque de reflexión/amplificación de DNS - UDP/53

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	5.00 Kpps	326.82 Mbps	168.71 Mbps	32.73 Kpps	16.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	4.59 Mbps	3.21 Mbps	433.00 pps	305.56 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	4.33 Mbps	2.95 Mbps	516.00 pps	366.67 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	203.42 Mbps	101.67 Mbps	20.15 Kpps	10.10 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	114.55 Mbps	83.22 Mbps	11.63 Kpps	8.37 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

Ataque de reflexión/amplificación de DNS - UDP/53

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	5.00 Kpps	326.82 Mbps	168.71 Mbps	32.73 Kpps	16.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	4.59 Mbps	3.21 Mbps	433.00 pps	305.56 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	4.33 Mbps	2.95 Mbps	516.00 pps	366.67 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	203.42 Mbps	101.67 Mbps	20.15 Kpps	10.10 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	114.55 Mbps	83.22 Mbps	11.63 Kpps	8.37 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

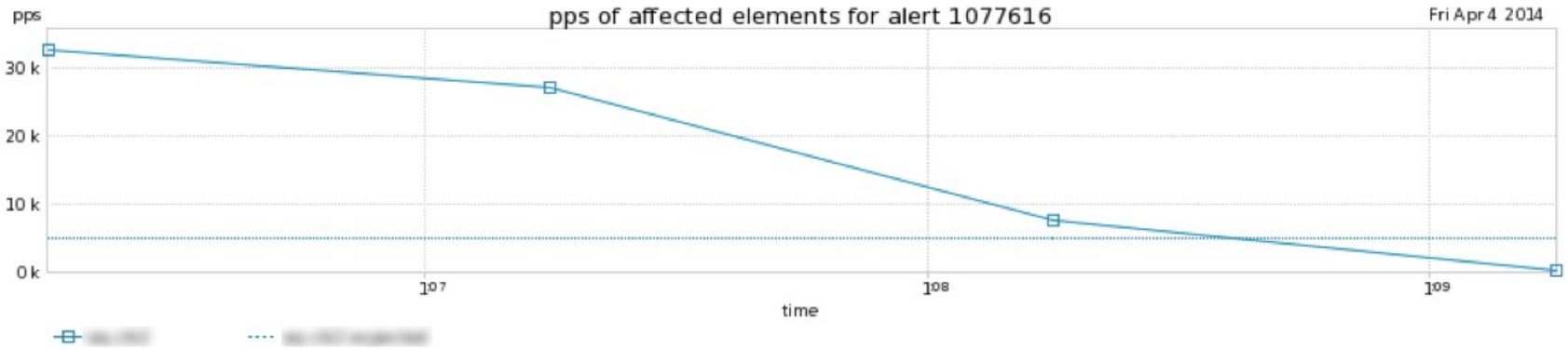
Ataque de reflexión/amplificación de DNS - UDP/53

DoS Alert 1077616 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1077616	High 328.3% Of 10.0 Kpps	329.64 Mbps 32.39 Kpps	0:09 (Ended)	Fri, Apr 4 2014, 01:03:14	Incoming	UDP (Misuse)	DNS Reflected/Amplified Attack Traffic [redacted]/32 DNS Reflected/Amplified Attack Traffic



Ataque de reflexión/amplificación de DNS - UDP/53

Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	5.00 kpps	326.82 M	168.71 M	32.73 k	16.88 k

Change Timeframe

Timeframe:

Other (*Interval*) 2014-04-04 01:06:15 (*Start*) 2014-04-04 01:09:15 (*End*) Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
5.06 G	4.05 M	1.25 k	168.71 M	16.88 k

Ataque de reflexión/amplificación de DNS - UDP/53

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	997.64 M	826.00 k	1.21 k	33.25 M	3.44 k	20.40	☑
80.240.0.0/12 ?	888.50 M	705.00 k	1.26 k	29.62 M	2.94 k	17.41	☑
80.64.0.0/11 ?	888.15 M	647.00 k	1.37 k	29.60 M	2.70 k	15.98	☑
80.64.0.0/10 ?	438.96 M	385.00 k	1.14 k	14.63 M	1.60 k	9.51	☑
80.128.0.0/9 ?	359.47 M	265.00 k	1.36 k	11.98 M	1.10 k	6.54	☑
80.80.0.0/12 ?	344.24 M	256.00 k	1.34 k	11.47 M	1.07 k	6.32	☑
80.48.0.0/13 ?	350.93 M	247.00 k	1.42 k	11.70 M	1.03 k	6.10	☑
80.12.0.0/14 ?	251.94 M	246.00 k	1.02 k	8.40 M	1.02 k	6.07	☑
0.0.0.0/0 ?	276.77 M	241.00 k	1.15 k	9.23 M	1.00 k	5.95	☑
60.0.0.0/10 ?	264.85 M	232.00 k	1.14 k	8.83 M	966.67	5.73	☑

Ataque de reflexión/amplificación de DNS - UDP/53

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	997.64 M	826.00 k	1.21 k	33.25 M	3.44 k	20.40	☑
10.240.0.0/12 ?	888.50 M	705.00 k	1.26 k	29.62 M	2.94 k	17.41	☑
80.64.0.0/11 ?	888.15 M	647.00 k	1.37 k	29.60 M	2.70 k	15.98	☑
80.64.0.0/10 ?	438.96 M	385.00 k	1.14 k	14.63 M	1.60 k	9.51	☑
80.128.0.0/9 ?	359.47 M	265.00 k	1.36 k	11.98 M	1.10 k	6.54	☑
80.80.0.0/12 ?	344.24 M	256.00 k	1.34 k	11.47 M	1.07 k	6.32	☑
80.48.0.0/13 ?	350.93 M	247.00 k	1.42 k	11.70 M	1.03 k	6.10	☑
80.12.0.0/14 ?	251.94 M	246.00 k	1.02 k	8.40 M	1.02 k	6.07	☑
0.0.0.0/0 ?	276.77 M	241.00 k	1.15 k	9.23 M	1.00 k	5.95	☑
60.0.0.0/10 ?	264.85 M	232.00 k	1.14 k	8.83 M	966.67	5.73	☑

Ataque de reflexión/amplificación de DNS - UDP/53

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	997.64 M	826.00 k	1.21 k	33.25 M	3.44 k	20.40	☑
80.240.0.0/12 ?	888.50 M	705.00 k	1.26 k	29.62 M	2.94 k	17.41	☑
80.64.0.0/11 ?	888.15 M	647.00 k	1.37 k	29.60 M	2.70 k	15.98	☑
80.64.0.0/10 ?	438.96 M	385.00 k	1.14 k	14.63 M	1.60 k	9.51	☑
80.128.0.0/9 ?	359.47 M	265.00 k	1.36 k	11.98 M	1.10 k	6.54	☑
80.80.0.0/12 ?	344.24 M	256.00 k	1.34 k	11.47 M	1.07 k	6.32	☑
80.48.0.0/13 ?	350.93 M	247.00 k	1.42 k	11.70 M	1.03 k	6.10	☑
80.12.0.0/14 ?	251.94 M	246.00 k	1.02 k	8.40 M	1.02 k	6.07	☑
0.0.0.0/0 ?	276.77 M	241.00 k	1.15 k	9.23 M	1.00 k	5.95	☑
60.0.0.0/10 ?	264.85 M	232.00 k	1.14 k	8.83 M	966.67	5.73	☑

Ataque de reflexión/amplificación de DNS - UDP/53

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
domain (53)	udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
13671	udp (17)	67.00 k	1.00 k	67.00	2.23 k	4.17	0.02	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ataque de reflexión/amplificación de DNS - UDP/53

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
domain (53)	udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
13671	udp (17)	67.00 k	1.00 k	67.00	2.23 k	4.17	0.02	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ataque de reflexión/amplificación de DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ataque de reflexión/amplificación de DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ataque de reflexión/amplificación de DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ataque de reflexión/amplificación de DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

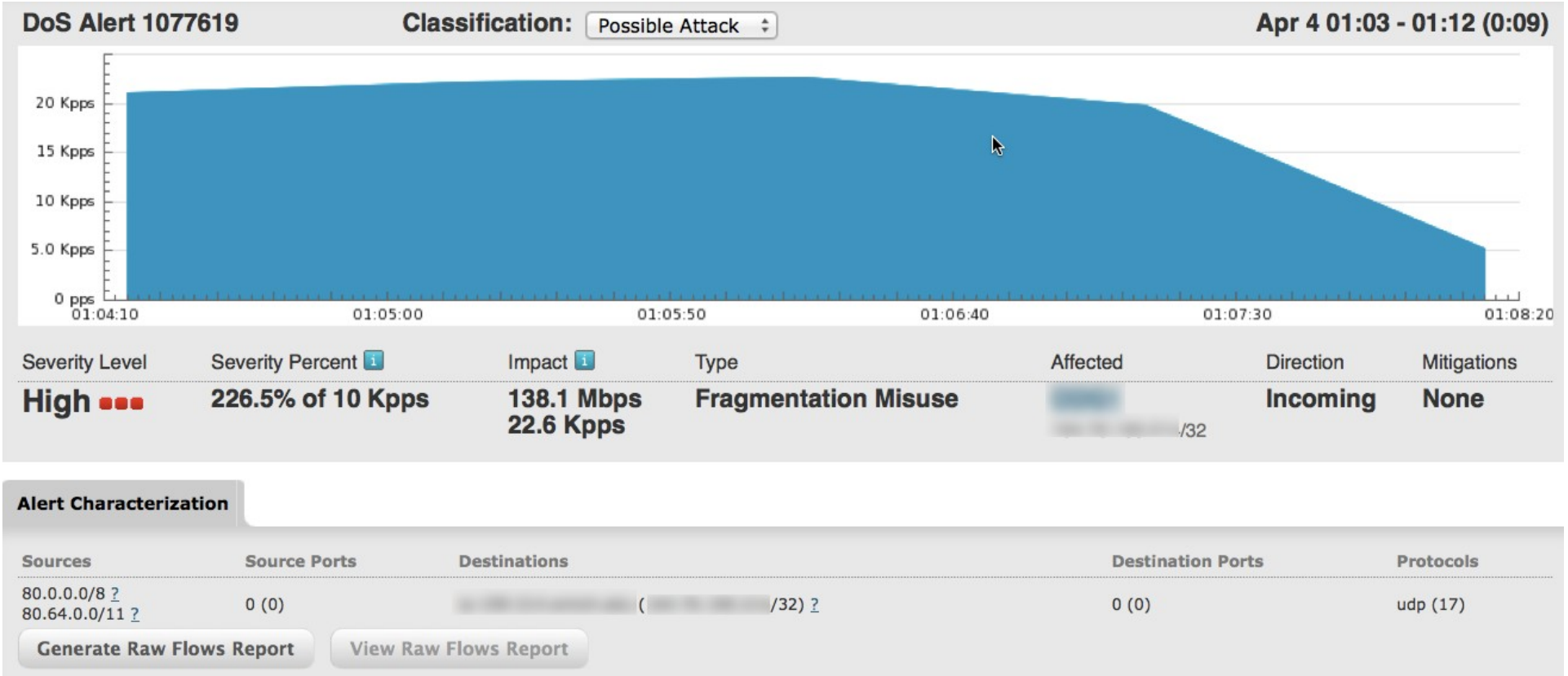
Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

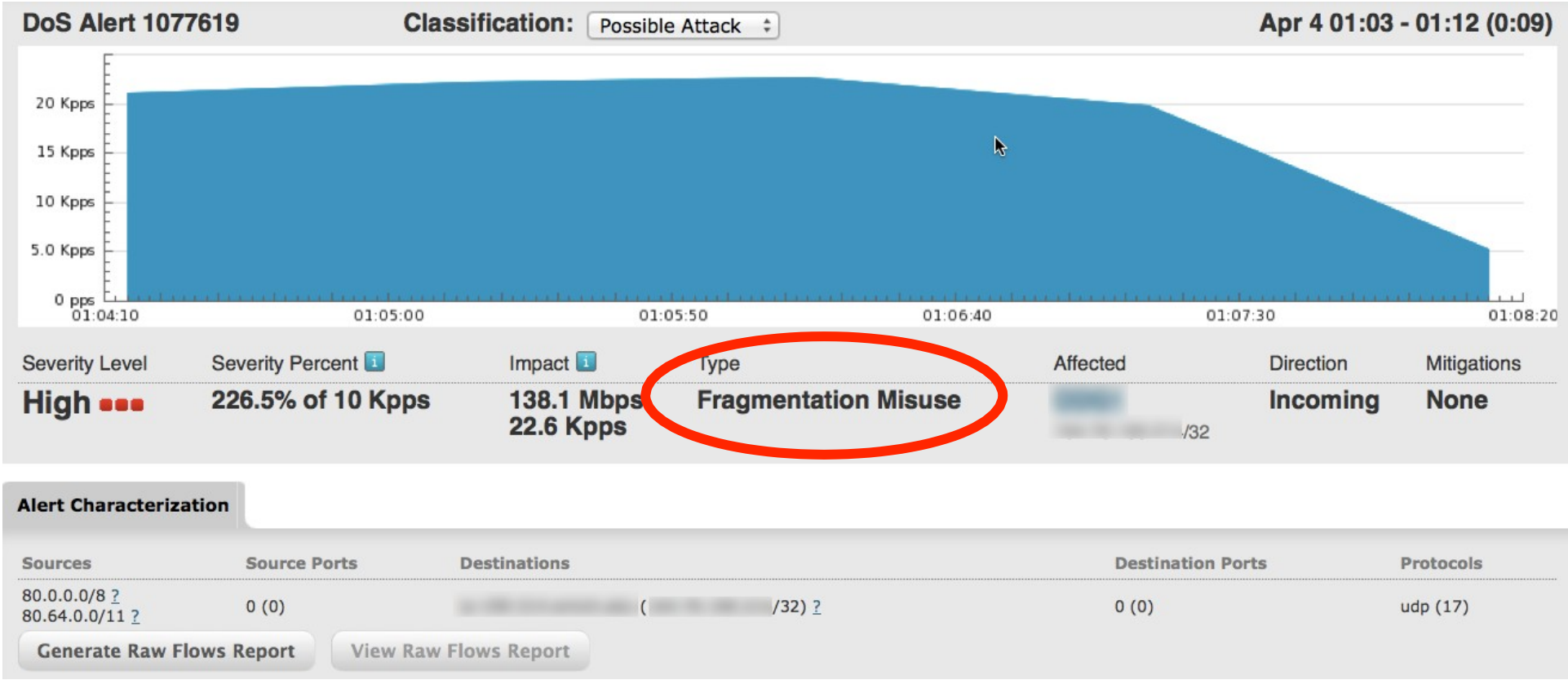
Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales



Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales



Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router	High	2.00 Kpps	137.70 Mbps	96.15 Mbps	22.58 Kpps	15.86 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	55.11 Mbps	40.16 Mbps	8.92 Kpps	6.58 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	2.00 Kpps	137.70 Mbps	96.15 Mbps	22.58 Kpps	15.86 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	55.11 Mbps	40.16 Mbps	8.92 Kpps	6.58 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router	High	2.00 Kpps	137.70 Mbps	96.15 Mbps	22.58 Kpps	15.86 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	55.11 Mbps	40.16 Mbps	8.92 Kpps	6.58 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

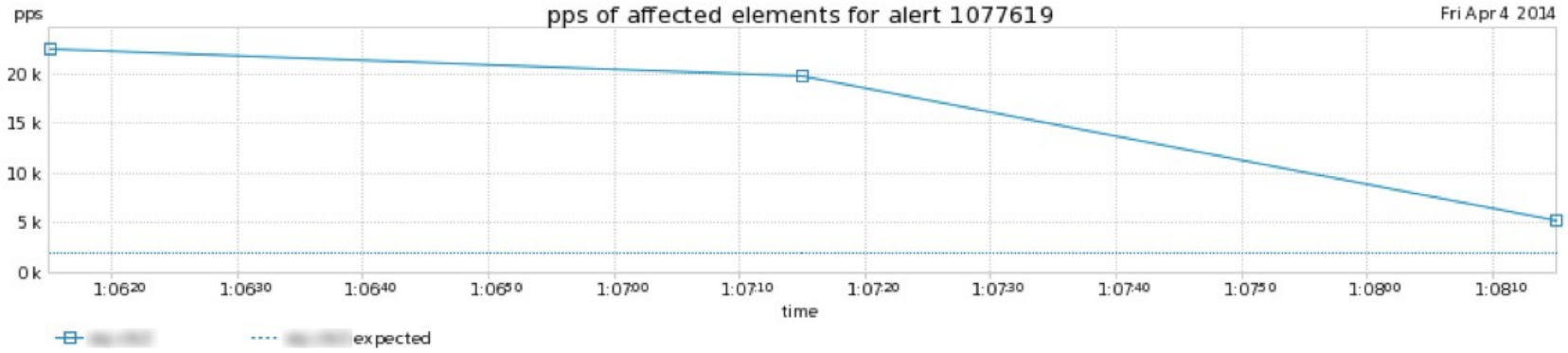
Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

DoS Alert 1077619 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1077619	High 226.5% Of 10.0 Kpps	138.10 Mbps 22.65 Kpps	0:09 (Ended)	Fri, Apr 4 2014, 01:03:14	Incoming	Fragment (Misuse)	[redacted]/32



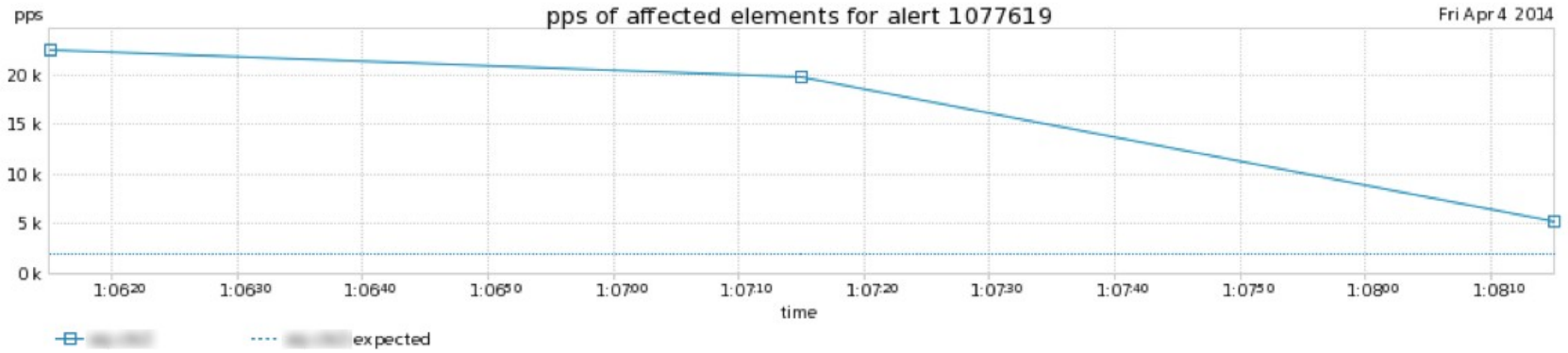
Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

DoS Alert 1077619 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1077619	High 226.5% Of 10.0 Kpps	138.10 Mbps 22.65 Kpps	0:09 (Ended)	Fri, Apr 4 2014, 01:03:14	Incoming	Fragment (Misuse)	[redacted]/32



Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	2.00 kpps	137.70 M	96.15 M	22.58 k	15.86 k

Change Timeframe

Timeframe:

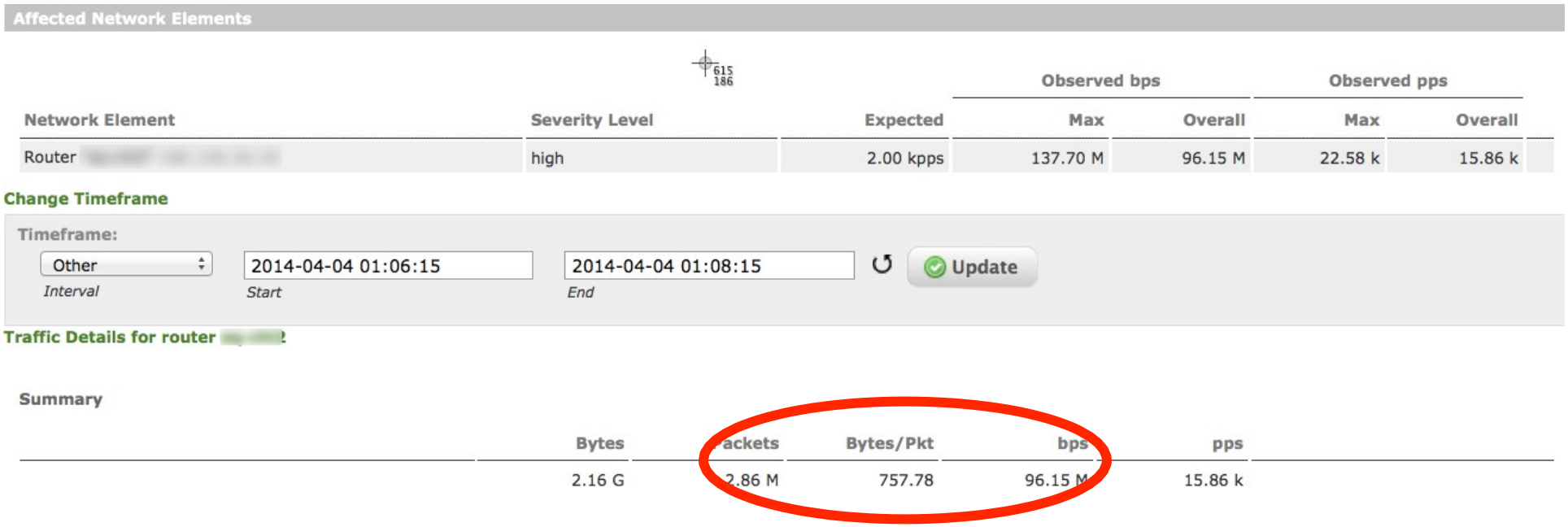
Other (*Interval*) | 2014-04-04 01:06:15 (*Start*) | 2014-04-04 01:08:15 (*End*) | Update

Traffic Details for router [redacted]

Summary

	Bytes	Packets	Bytes/Pkt	bps	pps
	2.16 G	2.86 M	757.78	96.15 M	15.86 k

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	2.00 kpps	137.70 M	96.15 M	22.58 k	15.86 k

Change Timeframe

Timeframe: Other (Interval) | 2014-04-04 01:06:15 (Start) | 2014-04-04 01:08:15 (End) | Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
2.16 G	2.86 M	757.78	96.15 M	15.86 k

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	432.54 M	612.00 k	706.76	19.22 M	3.40 k	21.44	☑
80.64.0.0/11 ?	385.48 M	467.00 k	825.44	17.13 M	2.59 k	16.36	☑
0.0.0.0/0 ?	290.26 M	424.00 k	684.58	12.90 M	2.36 k	14.85	☑
80.240.0.0/12 ?	281.81 M	399.00 k	706.29	12.52 M	2.22 k	13.98	☑
80.0.0.0/9 ?	303.92 M	379.00 k	801.89	13.51 M	2.11 k	13.27	☑
80.80.0.0/12 ?	206.59 M	244.00 k	846.66	9.18 M	1.36 k	8.55	☑
80.128.0.0/9 ?	128.22 M	170.00 k	754.24	5.70 M	944.44	5.95	☑
80.232.0.0/13 ?	134.64 M	160.00 k	841.51	5.98 M	888.89	5.60	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	432.54 M	612.00 k	706.76	19.22 M	3.40 k	21.44	☑
80.64.0.0/11 ?	385.48 M	467.00 k	825.44	17.13 M	2.59 k	16.36	☑
0.0.0.0/0 ?	290.26 M	424.00 k	684.58	12.90 M	2.36 k	14.85	☑
80.240.0.0/12 ?	281.81 M	399.00 k	706.29	12.52 M	2.22 k	13.98	☑
80.0.0.0/9 ?	303.92 M	379.00 k	801.89	13.51 M	2.11 k	13.27	☑
80.80.0.0/12 ?	206.59 M	244.00 k	846.66	9.18 M	1.36 k	8.55	☑
80.128.0.0/9 ?	128.22 M	170.00 k	754.24	5.70 M	944.44	5.95	☑
80.232.0.0/13 ?	134.64 M	160.00 k	841.51	5.98 M	888.89	5.60	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.	521	1.20 G	1.60 M	751.39	53.43 M	8.89 k	56.04	☑
xe-4/0/0.104	584	903.70 M	1.19 M	762.62	40.16 M	6.58 k	41.51	☑
xe-5/0/1.584	518	29.06 M	36.00 k	807.34	1.29 M	200.00	1.26	☐
xe-4/0/1.386	516	28.47 M	34.00 k	837.36	1.27 M	188.89	1.19	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.	521	1.20 G	1.60 M	751.39	53.43 M	8.89 k	56.04	☑
xe-4/0/0.104	584	903.70 M	1.19 M	762.62	40.16 M	6.58 k	41.51	☑
xe-5/0/1.584	518	29.06 M	36.00 k	807.34	1.29 M	200.00	1.26	☐
xe-4/0/1.386	516	28.47 M	34.00 k	837.36	1.27 M	188.89	1.19	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Ataque de reflexión/amplificación de DNS - Fragmentos no iniciales

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.	521	1.20 G	1.60 M	751.39	53.43 M	8.89 k	56.04	☑
xe-4/0/0.104	584	903.70 M	1.19 M	762.62	40.16 M	6.58 k	41.51	☑
xe-5/0/1.584	518	29.06 M	36.00 k	807.34	1.29 M	200.00	1.26	☐
xe-4/0/1.386	516	28.47 M	34.00 k	837.36	1.27 M	188.89	1.19	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Reflección/Amplificación SNMP

Factor de amplificación - SNMP

Abreviatura	Protocolo	Puertos	Factor de Ampliación	# Servidores Abusables
CHARGEN	Protocolo de generación de personajes	UDP / 19	18x/1000x	Decenas de miles (90K)
DNS	Sistema de nombres de dominio	UDP / 53	160x	Millones (27M)
NTP	Protocolo de tiempo de red	UDP / 123	1000x	Más de cien mil (119K)
SNMP	Protocolo simple de gestión de redes	UDP / 161	880x	Millones (5M)
SSDP	Protocolo simple de descubrimiento de servicios	UDP /1900	20x/83x	Millones (2M)

Características de un ataque de reflexión/amplificación de SNMP

- El atacante falsifica la dirección IP del objetivo del ataque, envía una consulta SNMP *GetBulkRequest* a servicios SNMP abusivos que se ejecutan en dispositivos CPE domésticos, grandes routers de ISP y empresas, servidores, etc. Estos paquetes suelen tener una longitud de etc. entre 60 y 102 bytes
- El atacante elige el puerto UDP al que quiere dirigirse -puede ser cualquier puerto a elección del atacante- y lo utiliza como origen port. El puerto de destino es UDP/ 161.
- Los servicios SNMP "responden" al objetivo del ataque con flujos de paquetes de 423 bytes - 1560 bytes procedentes de UDP/161; el puerto de destino es el puerto de origen que el atacante eligió al generar las consultas SNMP.

Características de un ataque de reflexión/amplificación de SNMP (cont.)

- A medida que estos múltiples flujos de respuestas SNMP convergen, el volumen de ataque puede ser muy grande - el mayor ataque verificado de este tipo hasta ahora es de más de 60gb/sec. 20-30gb/seg. los ataques son comunes.
- Debido al gran volumen de los ataques, el ancho de banda de tránsito de Internet del objetivo, junto con el ancho de banda central de los pares/subidas del objetivo, así como el ancho de banda central de las redes intermediarias entre los diversos servicios SNMP de los que se está abusando y el objetivo, están saturados.
- Los atacantes más astutos enumerarán los identificadores de objetos (OID) individuales de SNMP en los servicios SNMP abusables, y enumerarán cada uno de ellos con queries lotes SNMP iterativos y falsificados queries. de fragmentos no iniciales en este escenario, a la manera de DNS.
- En la mayoría de los ataques, se aprovechan entre ~2.000-4.000 servicios SNMP abusables por attackers.Hasta 10.000 servicios SNMP se han observado en algunos ataques.

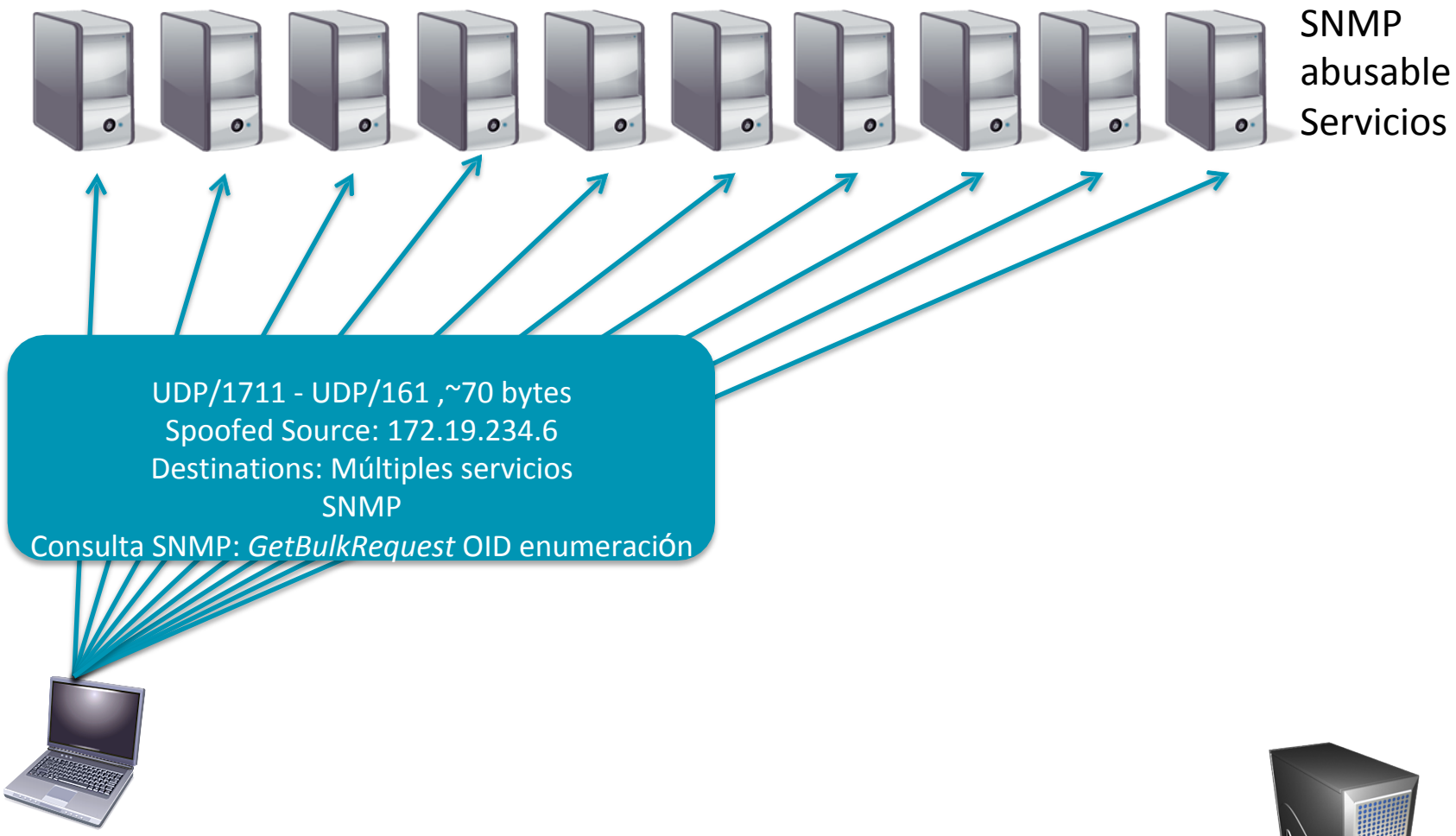
Metodología de ataque de reflexión/amplificación de SNMP

Internet--Servidores accesibles, routers, dispositivos CPE domésticos, etc.

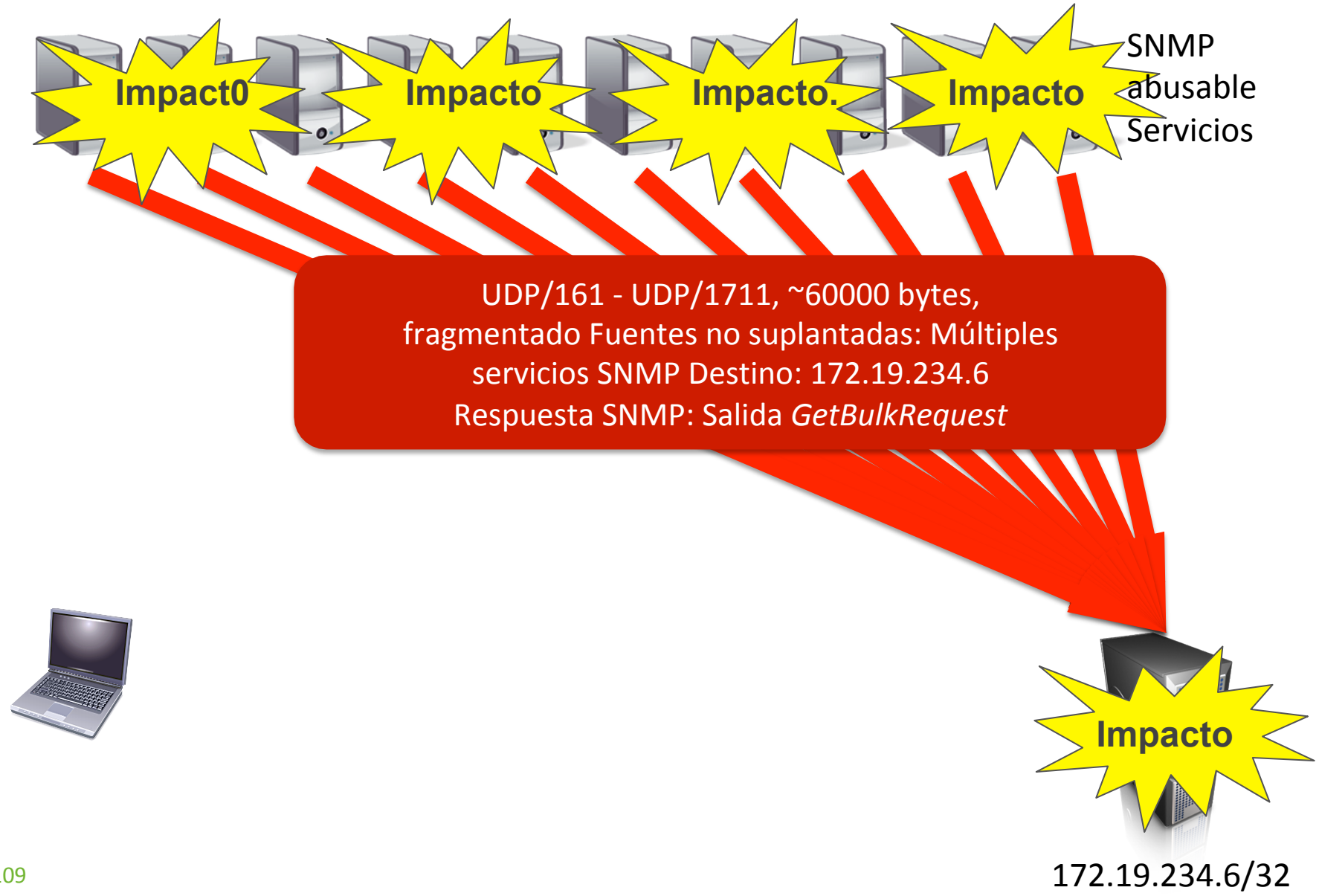
Internet-Accessible Servers, Routers, Home CPE devices, etc.

172.19.234.6/32

Metodología de ataque de reflexión/amplificación de SNMP



Metodología de ataque de reflexión/amplificación de SNMP



Carga Reflección/Amplificación

Factor de amplificación - chargen

Abreviatura	Protocolo	Puertos	Factor de Ampliación	# Servidores Abusables
CHARGEN	Protocolo de generación de personajes	UDP / 19	18x/1000x	Decenas de miles (90K)
DNS	Sistema de nombres de dominio	UDP / 53	160x	Millones (27M)
NTP	Protocolo de tiempo de red	UDP / 123	1000x	Más de cien mil (119K)
SNMP	Protocolo simple de gestión de redes	UDP / 161	880x	Millones (5M)
SSDP	Protocolo simple de descubrimiento de servicios	UDP /1900	20x/83x	Millones (2M)

Características de un ataque de reflexión/amplificación de la carga

- El atacante falsifica la dirección IP del objetivo del ataque, envía paquetes rellenos con al menos 18 bytes de carga útil (todo ceros; paquete de 70 bytes) a múltiples servicios de carga abusivos que se ejecutan en servidores, impresoras, dispositivos CPE domésticos, etc.
- El atacante elige el puerto UDP al que quiere dirigirse -puede ser cualquier puerto superior al 1023- y lo utiliza como origen port. El puerto de destino es UDP/19.
- queries. Los servicios de chargen 'responden' al objetivo del ataque con paquetes de ~1000- bytes - ~1500-bytes procedentes de UDP/19 hacia el objetivo; el puerto de destino es el puerto de origen que el atacante eligió cuando generó el chargen queries. La mayoría de los servicios de chargen generan un paquete de respuesta por cada paquete de solicitud, pero algunos servicios de chargen que no cumplen con la RFC envían más paquetes/consulta.

Características de un ataque de reflexión/amplificación de la carga (cont.)

- A medida que estos múltiples flujos de respuestas de carga convergen, el volumen de ataque puede ser bastante grande - el mayor ataque verificado de este tipo hasta el momento es de más de 137gb/sec. 2-5gb/seg ataques son comunes.
- Debido al gran volumen de los ataques, el ancho de banda de tránsito de Internet del objetivo, junto con el ancho de banda central de los pares/flujos ascendentes del objetivo, así como el ancho de banda central de las redes intermediarias entre los diversos servicios de carga de los que se está abusando y el objetivo, pueden saturarse.
- Los servicios de carga no conformes con la RFC pueden proporcionar un factor de amplificación de hasta 1000:1 (la mayoría son de 18:1).
- En la mayoría de los ataques, se aprovechan entre ~20 y ~2.000 servicios de carga abusivos por attackers. Hasta 5.000 servicios de carga se han observado en algunos ataques.

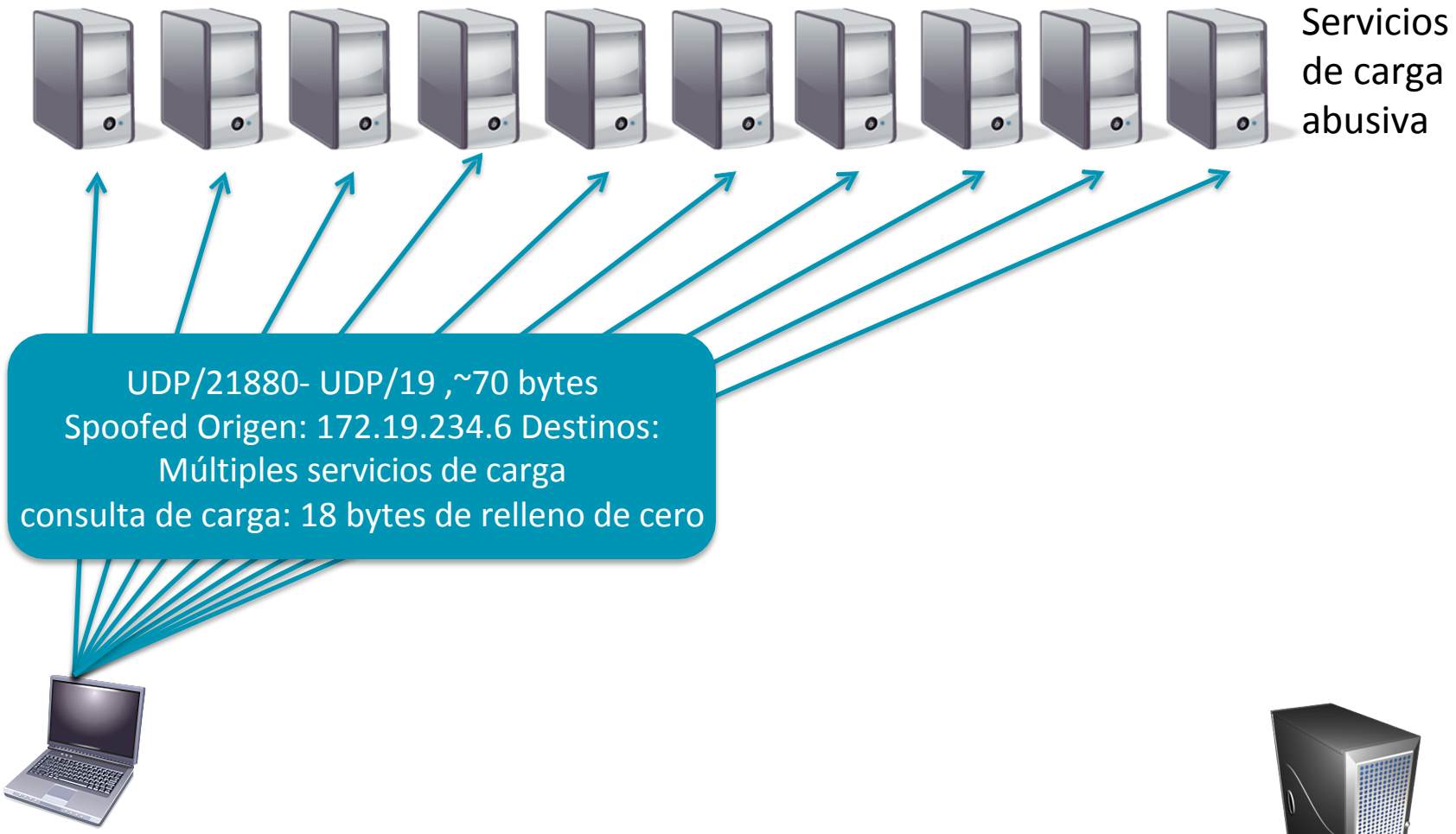
Metodología de ataque de reflexión/amplificación de la carga

Servicios de carga abusiva

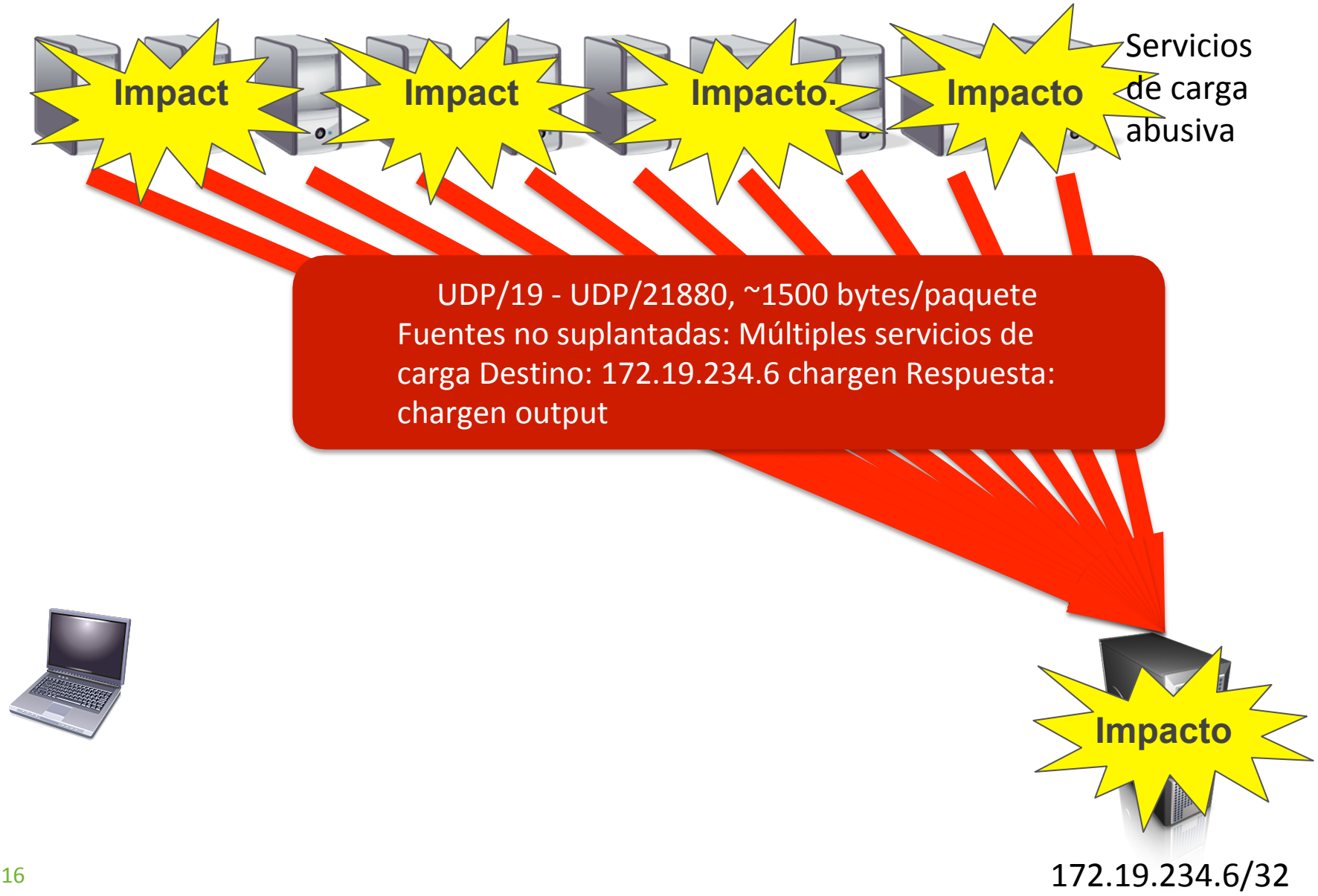
Internet--Servidores accesibles, routers, dispositivos CPE

172.19.234.6/32

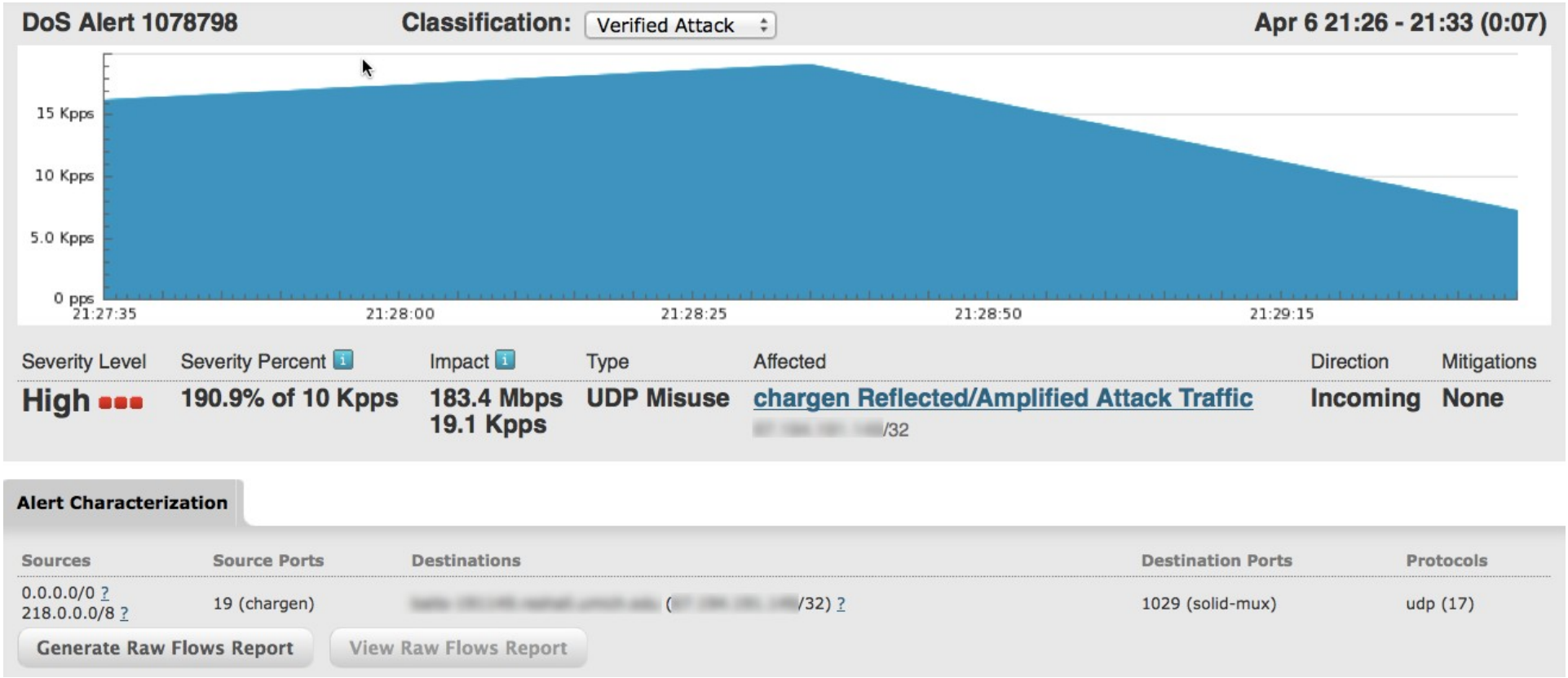
Metodología de ataque de reflexión/amplificación de la carga



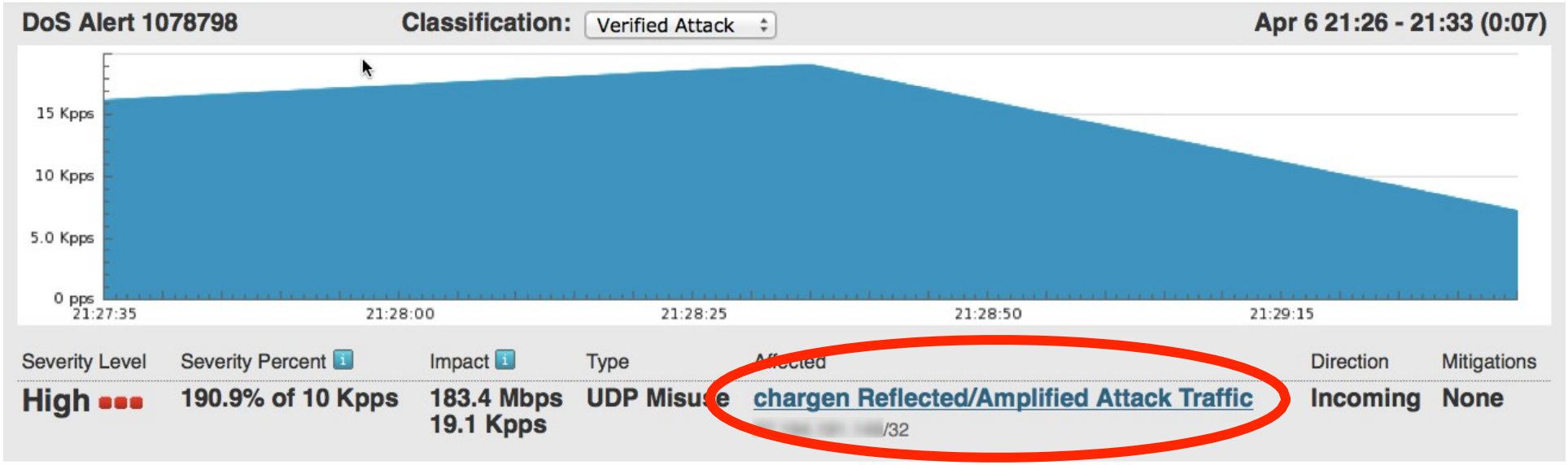
Metodología de ataque de reflexión/amplificación de la carga



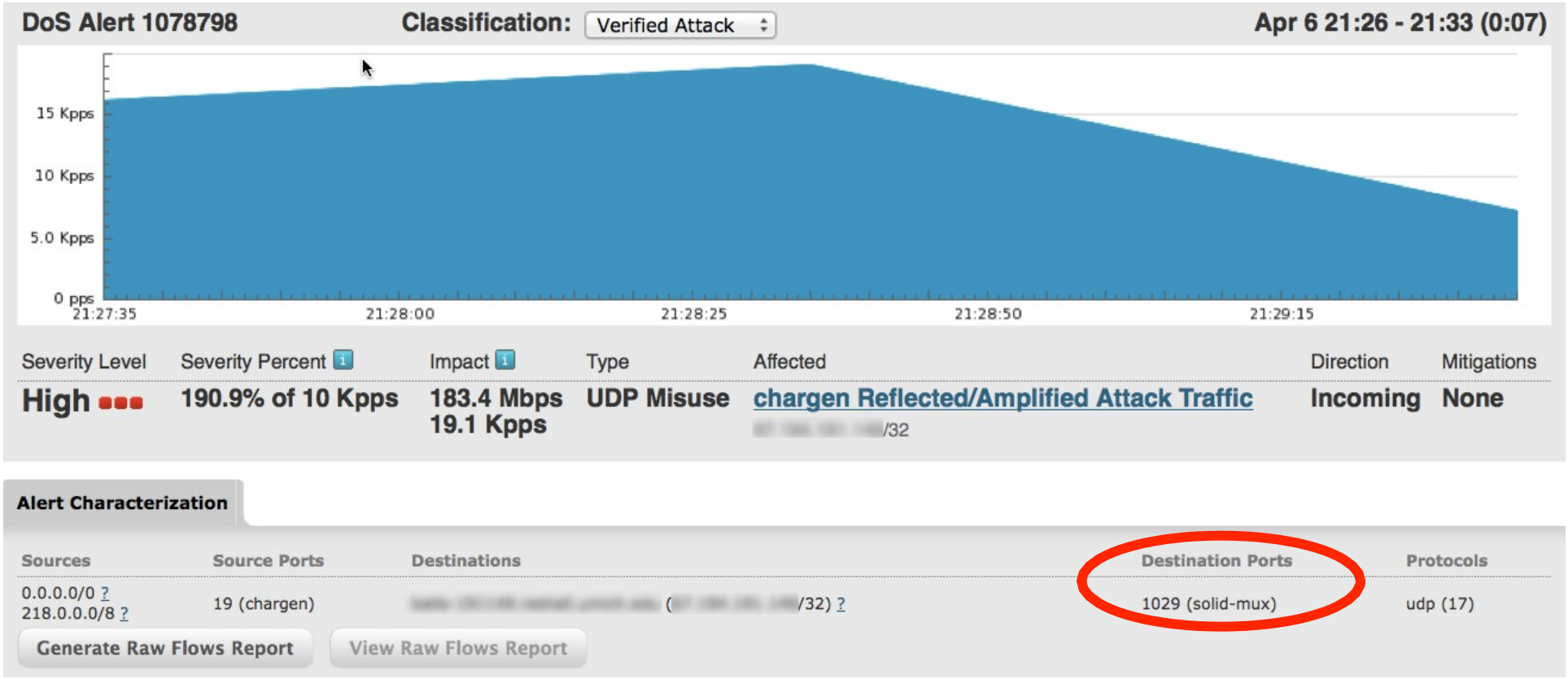
Ataque de reflexión/amplificación de la carga - UDP/19



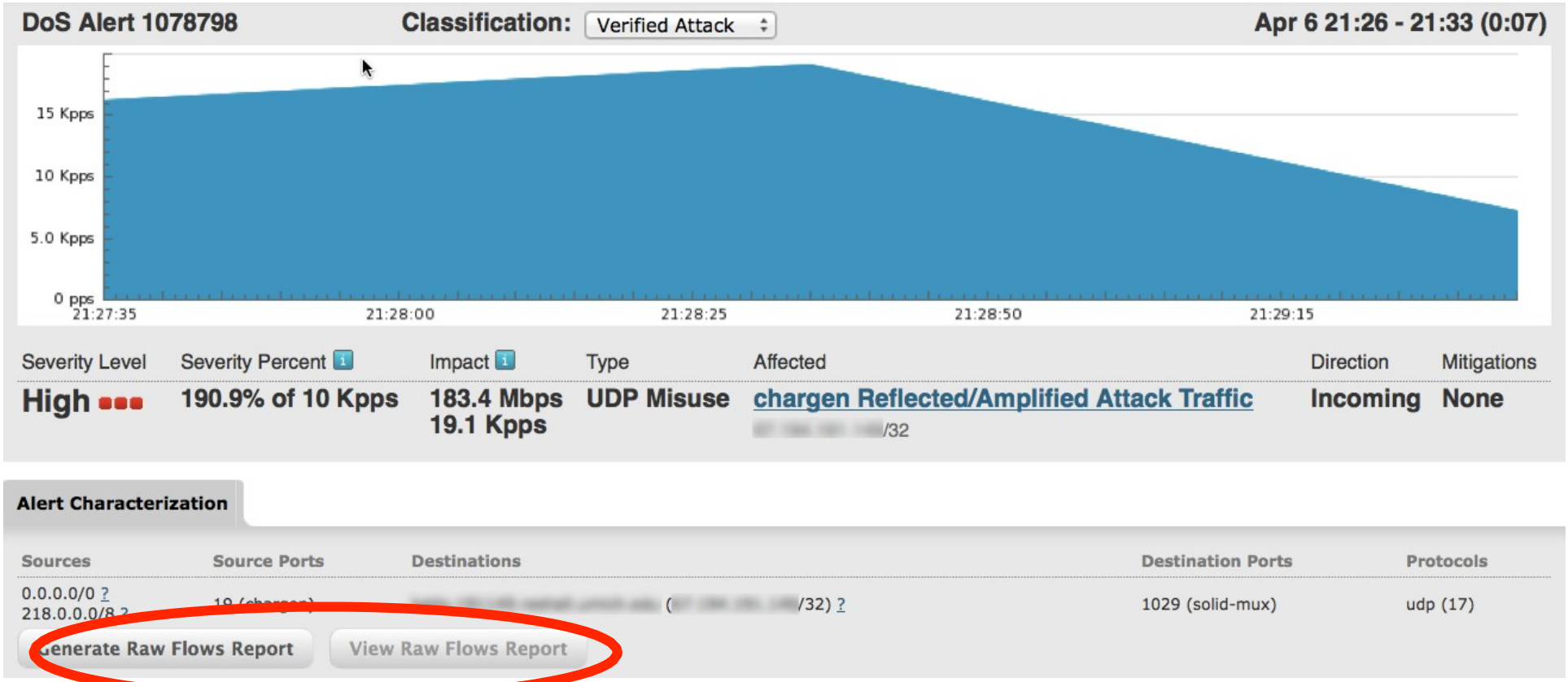
Ataque de reflexión/amplificación de la carga - UDP/19



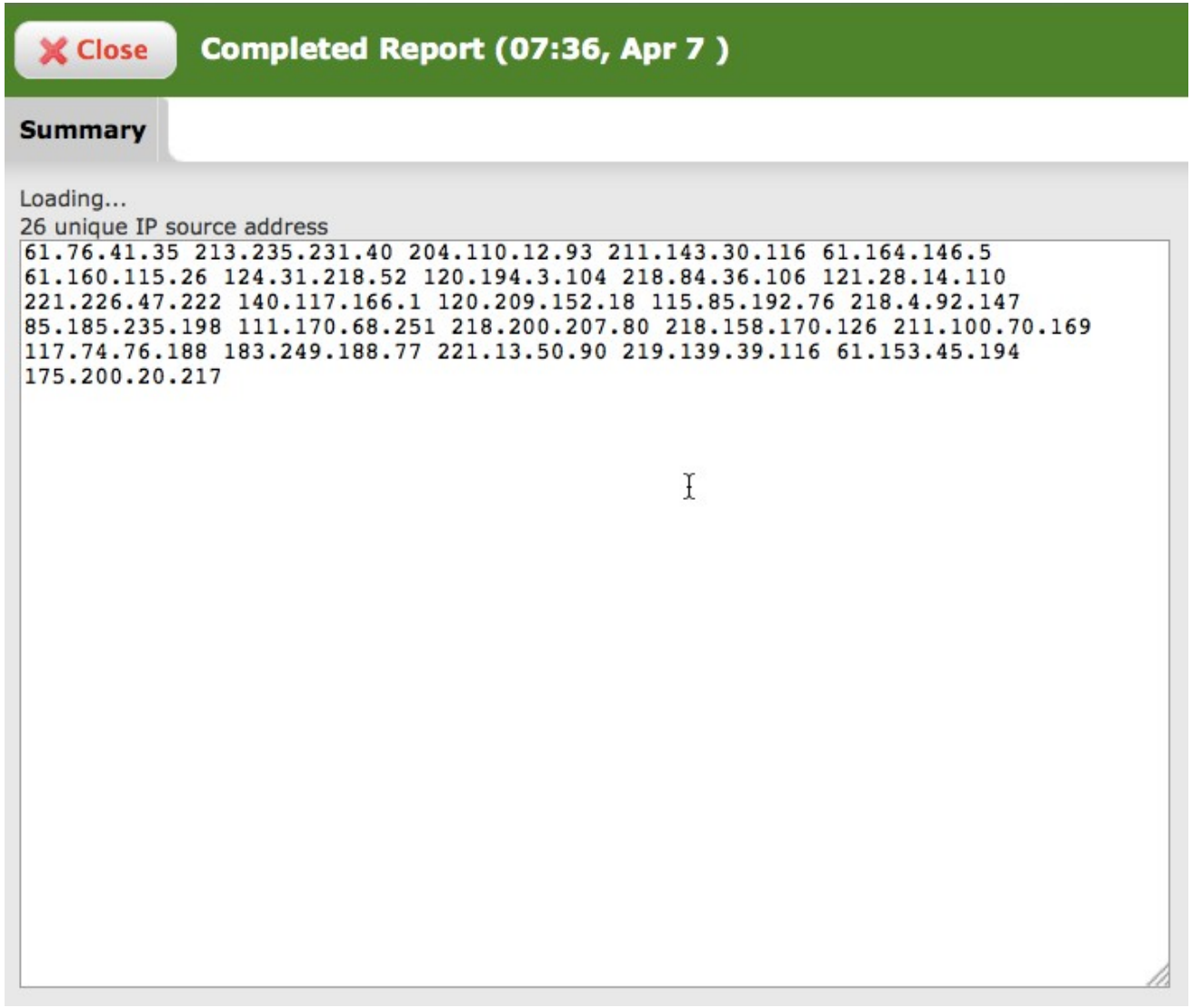
Ataque de reflexión/amplificación de la carga - UDP/19



Ataque de reflexión/amplificación de la carga - UDP/19



Ataque de reflexión/amplificación de la carga - UDP/19



Ataque de reflexión/amplificación de la carga - UDP/19

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router eq-chi2 [redacted]	High	5.00 Kpps	147.33 Mbps	73.92 Mbps	15.45 Kpps	7.76 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	500.13 Kbps	500.14 Kbps	50.00 pps	50.00 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	76.11 Mbps	38.15 Mbps	8.12 Kpps	4.07 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	49.96 Mbps	25.13 Mbps	5.10 Kpps	2.57 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	20.76 Mbps	10.38 Mbps	2.18 Kpps	1.10 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

chargen reflection/amplification attack.

Ataque de reflexión/amplificación de la carga - UDP/19

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router eq-chi2	High	5.00 Kpps	147.33 Mbps	73.92 Mbps	15.45 Kpps	7.16 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	500.13 Kbps	500.14 Kbps	50.00 pps	50.00 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	76.11 Mbps	38.15 Mbps	8.12 Kpps	4.07 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106		-	49.96 Mbps	25.13 Mbps	5.10 Kpps	2.57 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	20.76 Mbps	10.38 Mbps	2.18 Kpps	1.10 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

chargen reflection/amplification attack.

Ataque de reflexión/amplificación de la carga - UDP/19

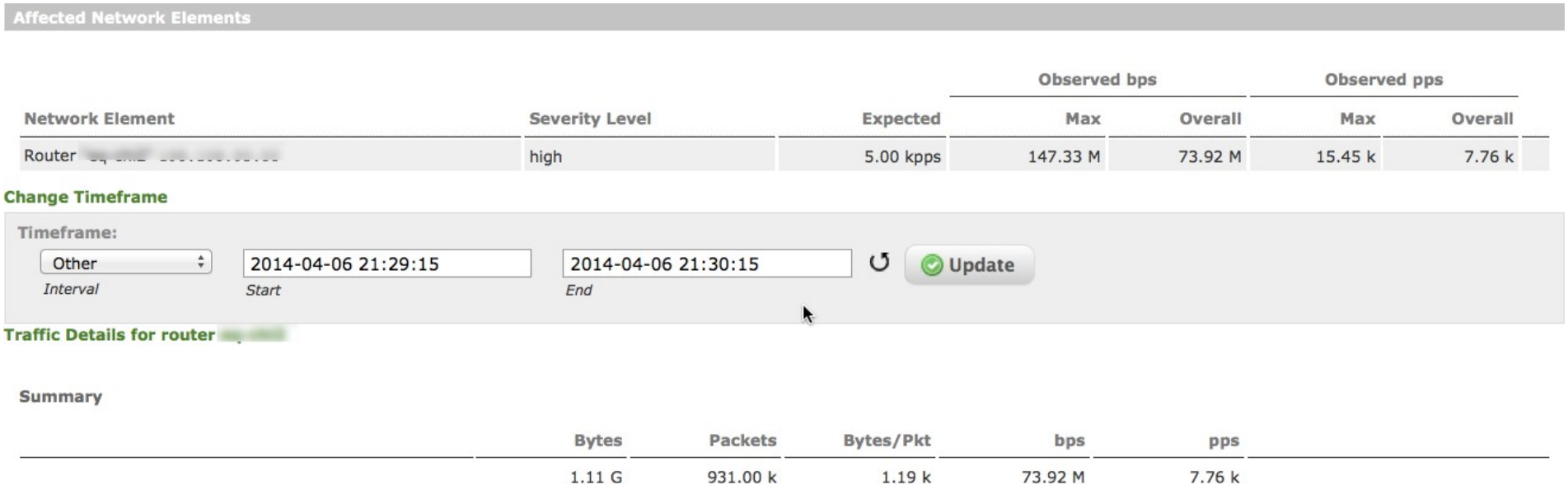
DoS Alert 1078798 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1078798	High 190.9% Of 10.0 Kpps	183.38 Mbps 19.09 Kpps	0:07 (Ended)	Sun, Apr 6 2014, 21:26:36	Incoming	UDP (Misuse)	chargen Reflected/Amplified Attack Traffic [redacted]/32 chargen Reflected/Amplified Attack Traffic

Ataque de reflexión/amplificación de la carga - UDP/19



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	5.00 kpps	147.33 M	73.92 M	15.45 k	7.76 k

Change Timeframe

Timeframe:

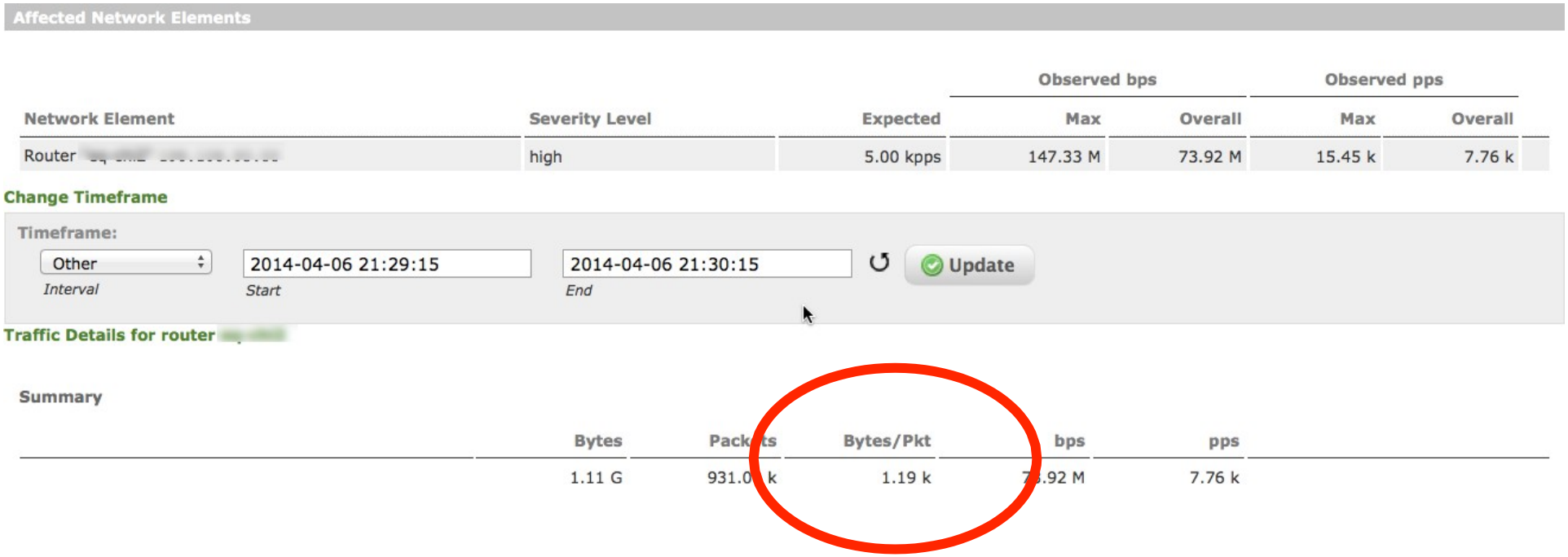
Other (*Interval*) | 2014-04-06 21:29:15 (*Start*) | 2014-04-06 21:30:15 (*End*) | Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
1.11 G	931.00 k	1.19 k	73.92 M	7.76 k

Ataque de reflexión/amplificación de la carga - UDP/19



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	5.00 kpps	147.33 M	73.92 M	15.45 k	7.76 k

Change Timeframe

Timeframe:

Other (*Interval*) | 2014-04-06 21:29:15 (*Start*) | 2014-04-06 21:30:15 (*End*) | Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
1.11 G	931.0 k	1.19 k	73.92 M	7.76 k

Ataque de reflexión/amplificación de la carga - UDP/19

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	940.18 M	792.00 k	1.19 k	62.68 M	6.60 k	85.07	☑
218.0.0.0/8 ?	108.55 M	91.00 k	1.19 k	7.24 M	758.33	9.77	☑
61.128.0.0/10 ?	60.03 M	48.00 k	1.25 k	4.00 M	400.00	5.16	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32) ?	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
chargen (19)	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1029	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ataque de reflexión/amplificación de la carga - UDP/19

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	940.18 M	792.00 k	1.19 k	62.68 M	6.60 k	85.07	☑
218.0.0.0/8 ?	108.55 M	91.00 k	1.19 k	7.24 M	758.33	9.77	☑
61.128.0.0/10 ?	60.03 M	48.00 k	1.25 k	4.00 M	400.00	5.16	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32) ?	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
chargen (19)	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1029	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ataque de reflexión/amplificación de la carga - UDP/19

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/0/1.584	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
xe-4/0/0.104	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-4/0/1.386	516	3.75 M	3.00 k	1.25 k	250.07 k	25.00	0.32	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ataque de reflexión/amplificación de la carga - UDP/19

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/0/1.584	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
xe-4/0/0.104	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-4/0/1.386	516	3.75 M	3.00 k	1.25 k	250.07 k	25.00	0.32	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ataque de reflexión/amplificación de la carga - UDP/19

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/0/1.584	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
xe-4/0/0.104	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-4/0/1.386	516	3.75 M	3.00 k	1.25 k	250.07 k	25.00	0.32	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Reflección/Amplificación del SSDP

Factor de amplificación - SSDP

Abreviatura	Protocolo	Puertos	Factor de Ampliación	# Servidores Abusables
CHARGEN	Protocolo de generación de personajes	UDP / 19	18x/1000x	Decenas de miles (90K)
DNS	Sistema de nombres de dominio	UDP / 53	160x	Millones (27M)
NTP	Protocolo de tiempo de red	UDP / 123	1000x	Más de cien mil (119K)
SNMP	Protocolo simple de gestión de redes	UDP / 161	880x	Millones (5M)
SSDP	Protocolo simple de descubrimiento de servicios	UDP /1900	20x/83x	Millones (2M)

Características de un ataque de reflexión/amplificación de SSDP

- El atacante falsifica la dirección IP del objetivo del ataque, envía una consulta SSDP *M-Search* a los servicios SSDP abusivos que se ejecutan en los dispositivos CPE domésticos y en algunos Windows XP antiguos systems Estos paquetes suelen tener una longitud de ~118 bytes.
- El atacante elige el puerto UDP al que quiere dirigirse -puede ser cualquier puerto a elección del atacante- y lo utiliza como origen port. El puerto de destino es UDP/ 1900.
- Los servicios SSDP "responden" al objetivo del ataque con flujos de paquetes de 1360 bytes - 9800 bytes procedentes de UDP/1900; el puerto de destino es el puerto de origen que el atacante eligió al generar el SSDP queries. Estos paquetes consistirán en fragmentos queries. UDP iniciales y no iniciales.

Características de un ataque de reflexión/amplificación de SSDP (cont.)

- A medida que estos múltiples flujos de respuestas SSDP convergen, el volumen de ataque puede ser muy grande - el mayor ataque verificado de este tipo hasta ahora es de más de 42gb/sec.10-35gb/seg. los ataques son comunes.
- Debido al gran volumen de los ataques, el ancho de banda de tránsito de Internet del objetivo, junto con el ancho de banda central de los pares/subidas del objetivo, así como el ancho de banda central de las redes intermediarias entre los diversos servicios SSDP de los que se abusa y el objetivo, están saturados.
- Los atacantes más astutos identificarán los servicios SSDP individuales disponibles en los dispositivos habilitados para SSDP que puedan ser objeto de abuso, y los enumerarán con queries. lotes SSDP falsos paralelos queries. de fragmentos no iniciales en este escenario, a la manera del DNS.
- En la mayoría de los ataques, se aprovechan entre ~4.000-6.000 servicios SSDP abusables por attackers. Hasta 10.000 servicios attackers. SSDP abusables se han observado en algunos ataques.

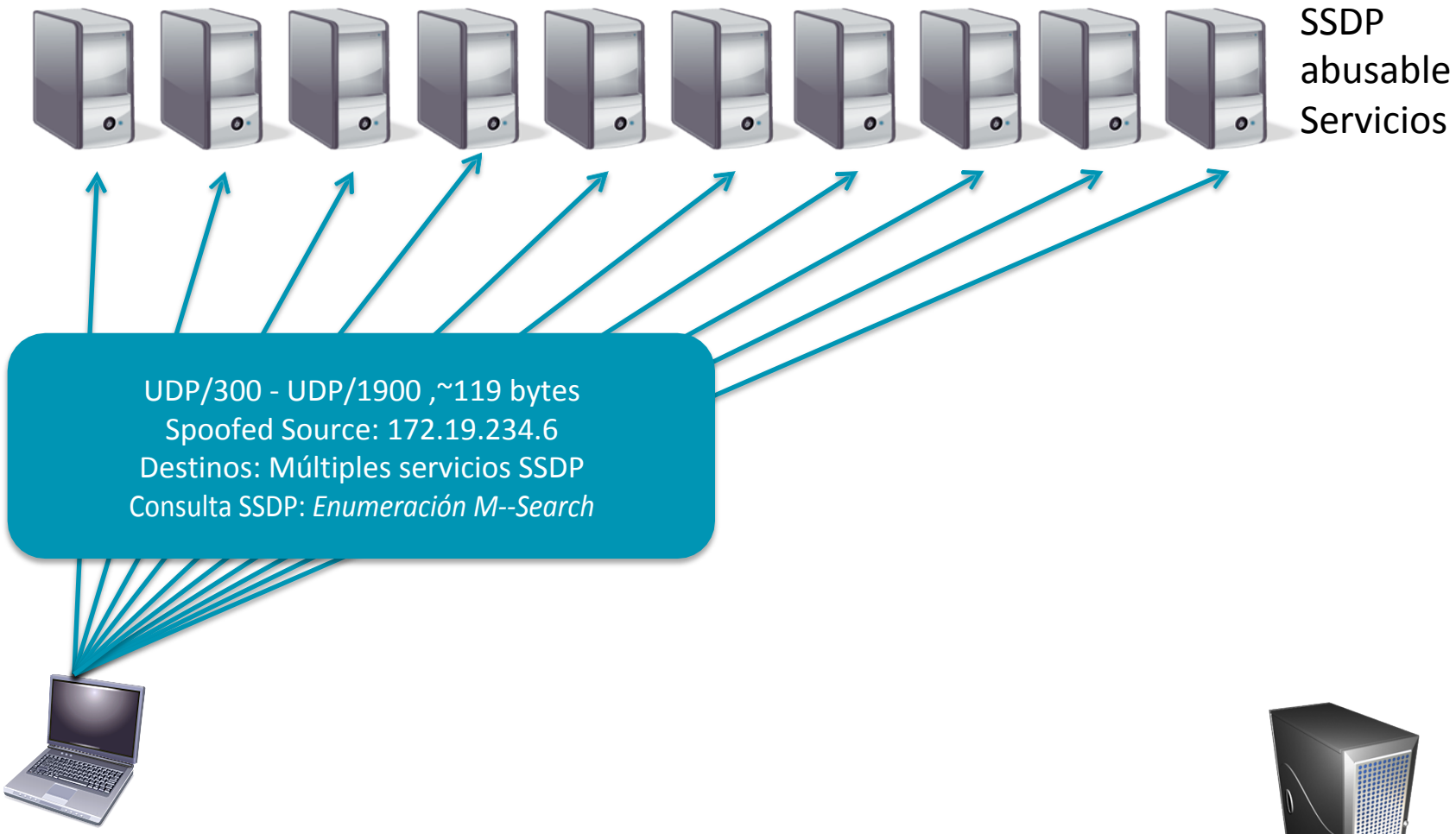
Metodología de ataque de reflexión/amplificación de SSDP

SSDP abusable Servicios

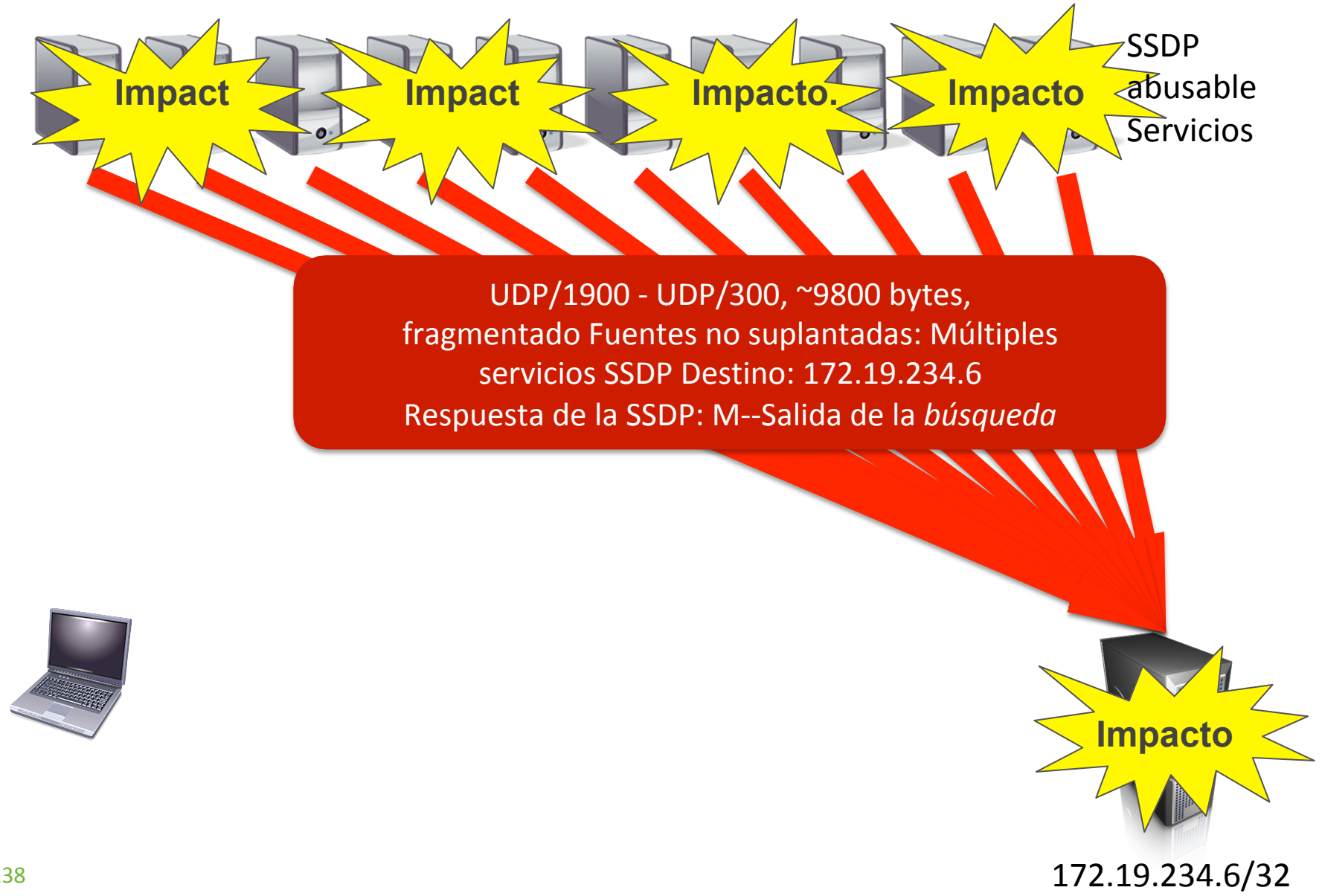
Dispositivos CPE accesibles a través de Internet, viejos equipos con Windows

172.19.234.6/32

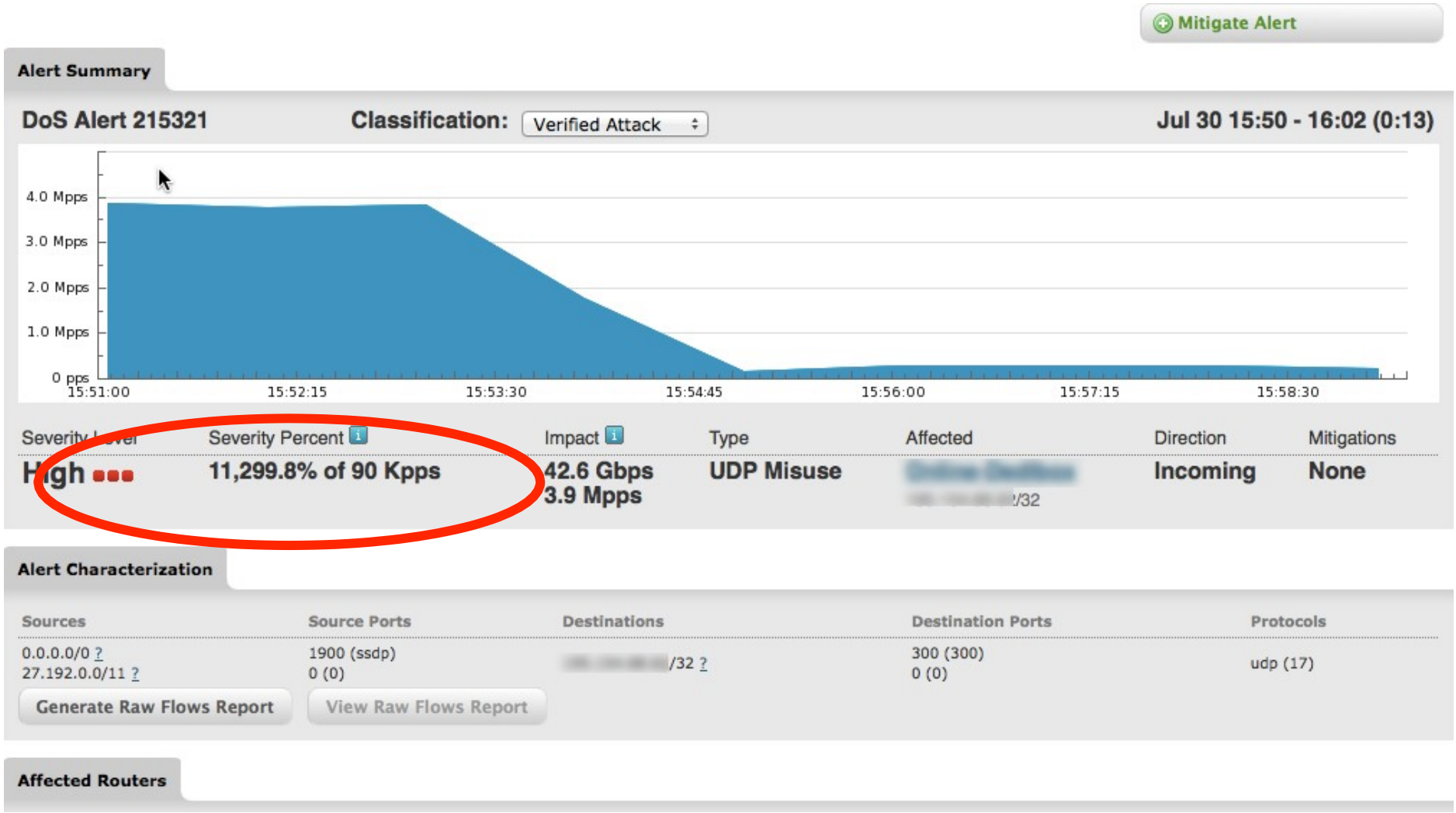
Metodología de ataque de reflexión/amplificación de SSDP



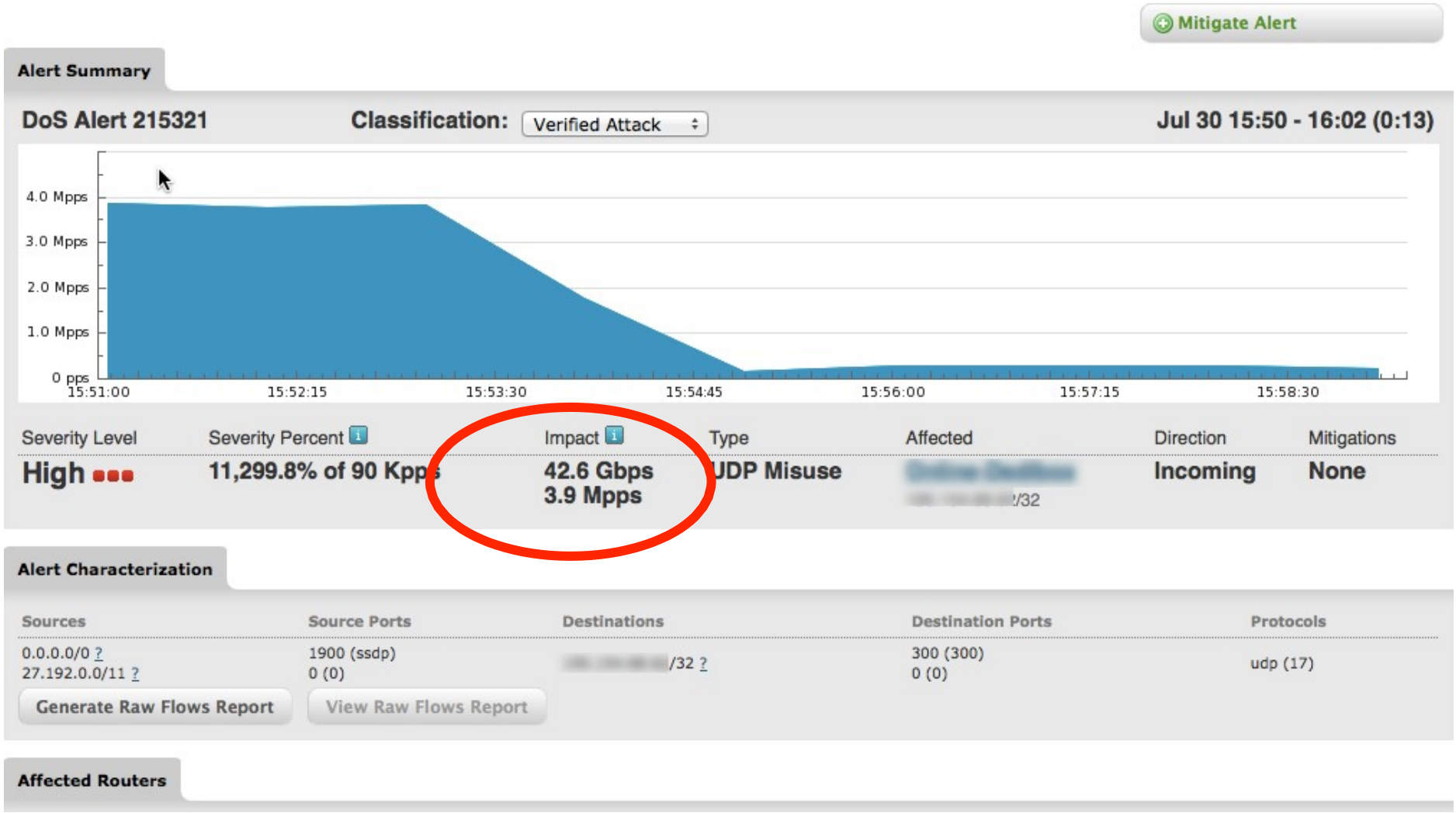
Metodología de ataque de reflexión/amplificación de SSDP



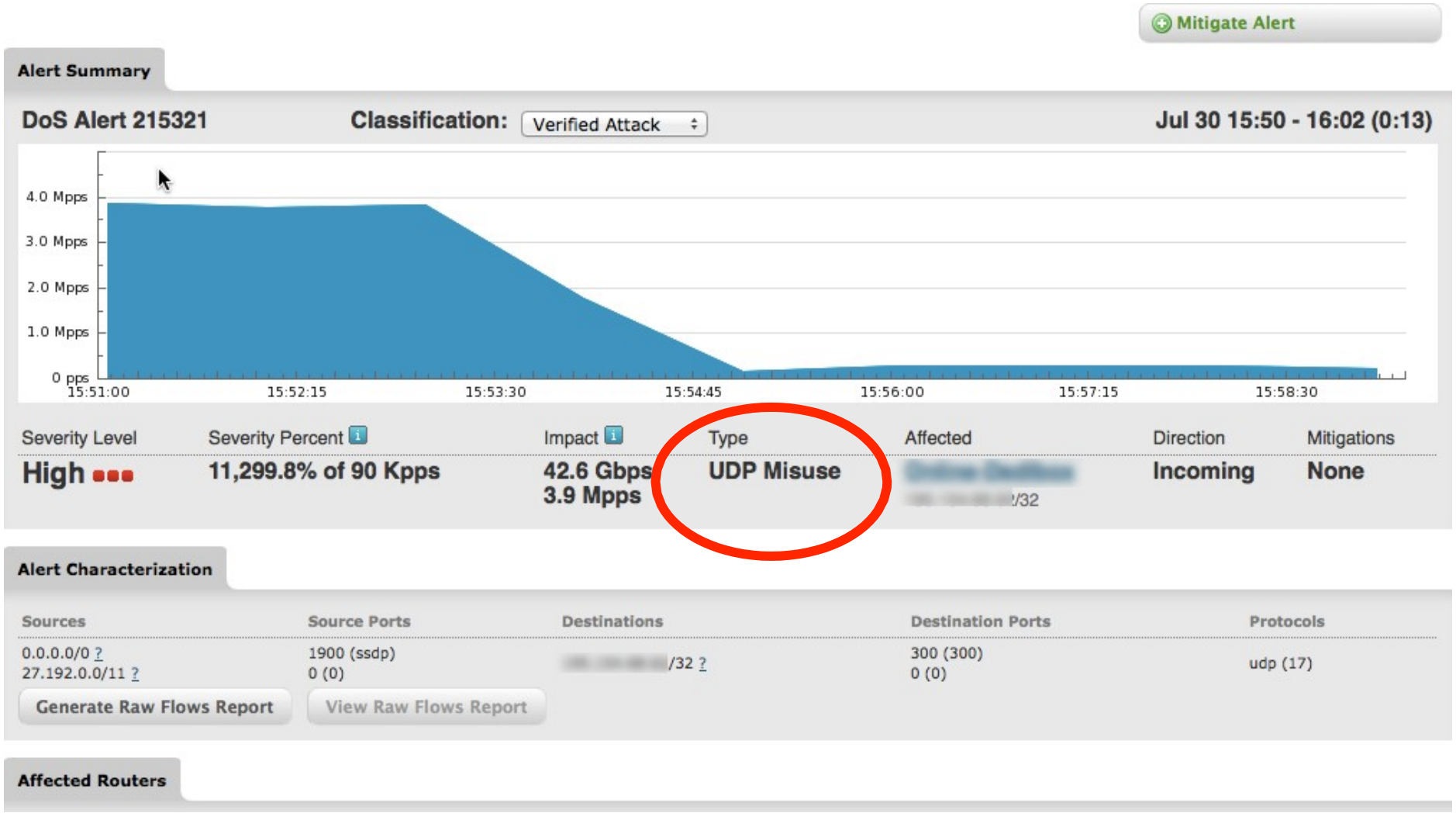
Ataque de reflexión/amplificación de SSDP



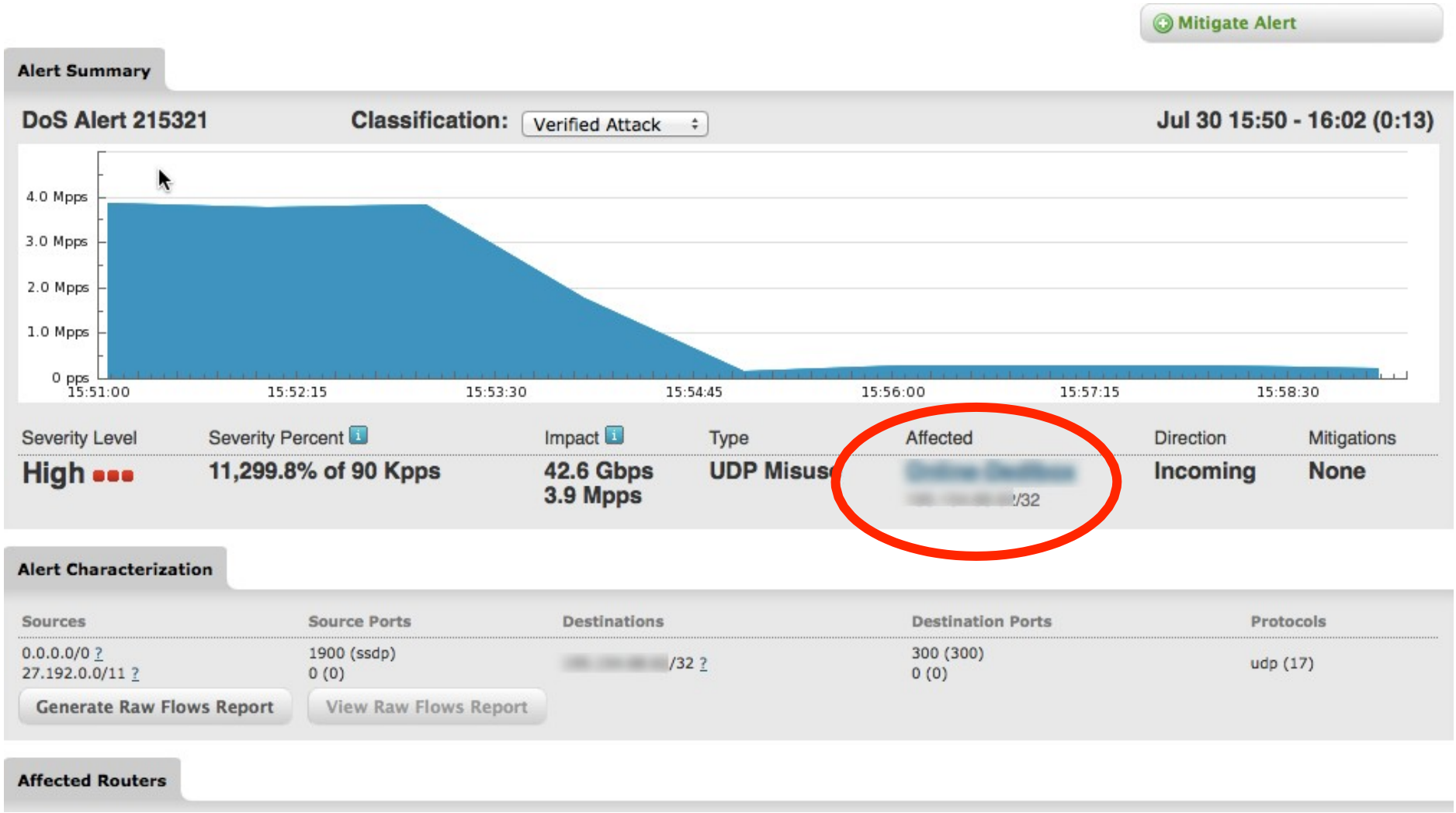
Ataque de reflexión/amplificación de SSDP



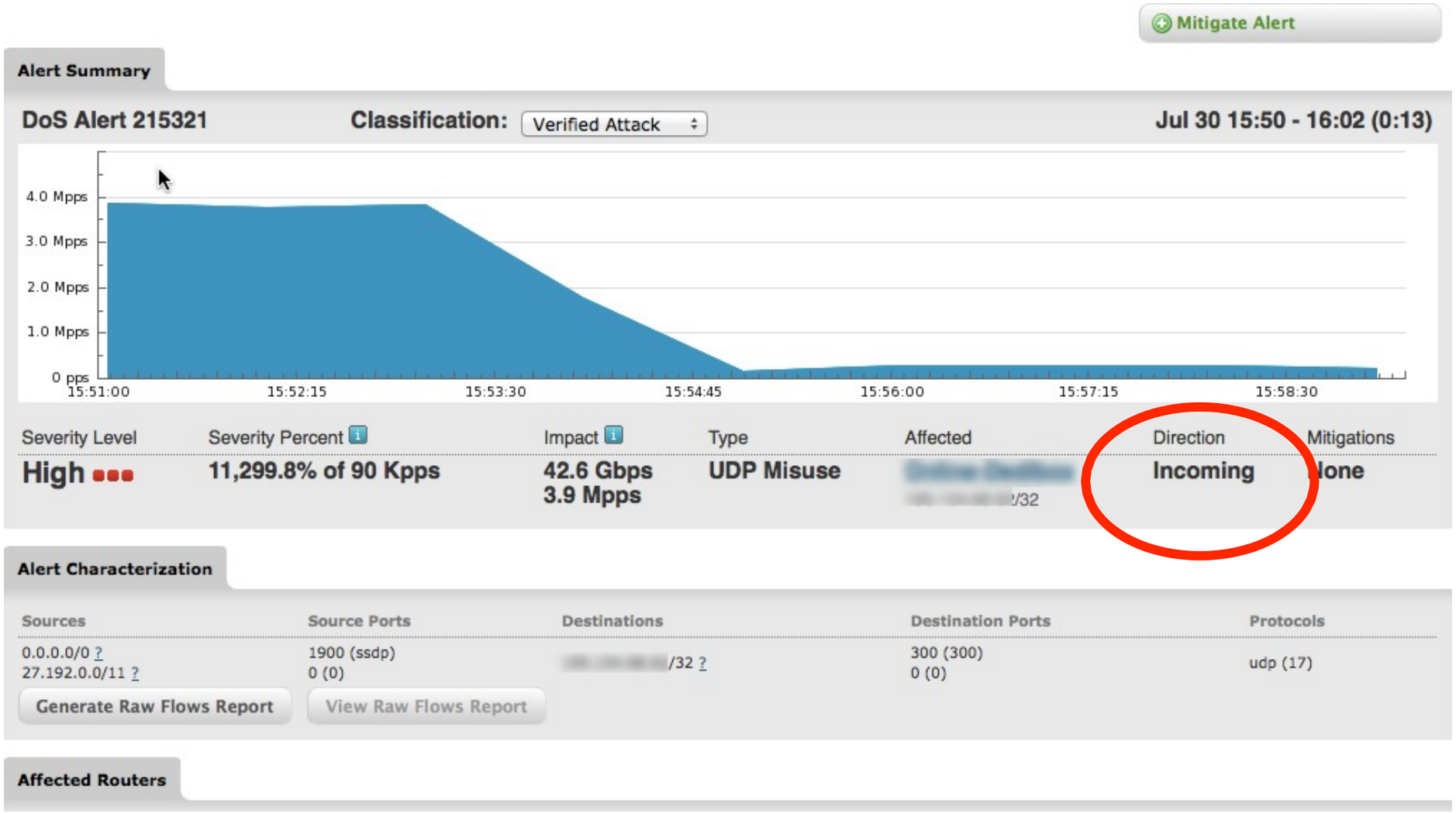
Ataque de reflexión/amplificación de SSDP



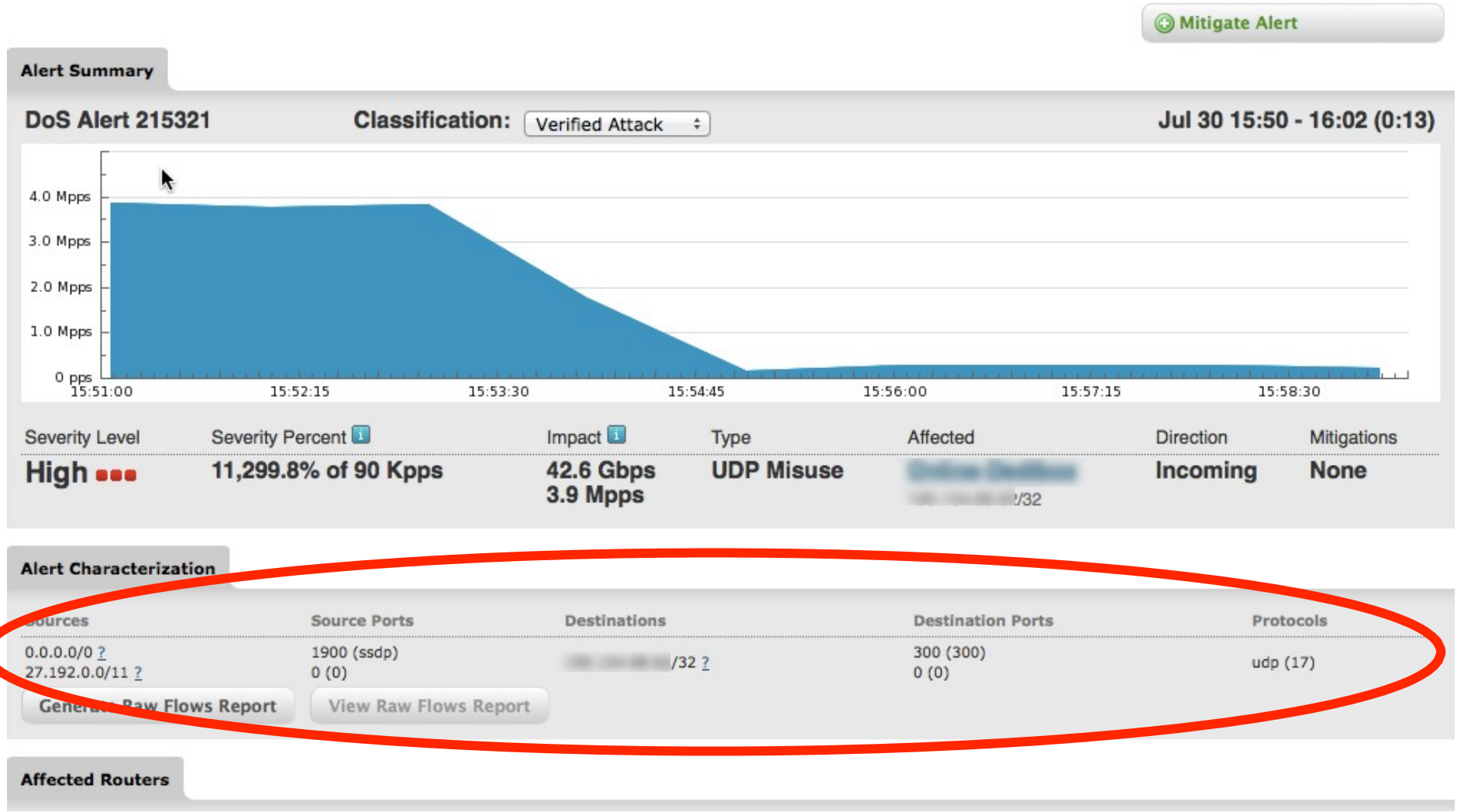
Ataque de reflexión/amplificación de SSDP



Ataque de reflexión/amplificación de SSDP



Ataque de reflexión/amplificación de SSDP



Ataque de reflexión/amplificación de SSDP

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	50.00 Kpps	40.14 Gbps	20.25 Gbps	9.94 Mpps	4.79 Mpps	Details
Interface (SNMP 315) Bundle-Ether2.1013		-	1.20 Gbps	549.60 Mbps	287.47 Kpps	166.81 Kpps	Details
Interface (SNMP 344) Bundle-Ether100.2002		-	3.89 Mbps	2.15 Mbps	1.48 Kpps	757.14 pps	Details
Interface (SNMP 299) Bundle-Ether6453		-	10.62 Gbps	3.70 Gbps	965.25 Kpps	559.58 Kpps	Details
Interface (SNMP 478) Bundle-Ether44530		-	5.40 Mbps	5.22 Mbps	533.00 pps	505.56 pps	Details
Interface (SNMP 480) Bundle-Ether1299		-	22.46 Gbps	14.26 Gbps	8.52 Mpps	3.83 Mpps	Details
Interface (SNMP 569) Bundle-Ether3356		-	4.96 Gbps	1.81 Gbps	448.37 Kpps	295.68 Kpps	Details
Interface (SNMP 626) Bundle-Ether3.4090		-	2.11 Gbps	792.03 Mbps	191.38 Kpps	90.91 Kpps	Details
Router	High	50.00 Kpps	2.24 Gbps	934.88 Mbps	294.82 Kpps	178.77 Kpps	Details
Interface (SNMP 88) TenGigE0/0/0/17		-	2.22 Mbps	1.78 Mbps	200.00 pps	155.56 pps	Details
Interface (SNMP 274) TenGigE0/0/0/11.4080		-	2.49 Mbps	1.76 Mbps	233.00 pps	161.11 pps	Details
Interface (SNMP 361) Bundle-Ether44530		-	12.51 Mbps	5.46 Mbps	1.12 Kpps	891.44 pps	Details
Interface (SNMP 445) Bundle-Ether3.4080		-	2.09 Gbps	787.81 Mbps	189.22 Kpps	90.86 Kpps	Details
Interface (SNMP 470) TenGigE0/4/0/20.4		-	634.94 Mbps	298.68 Mbps	244.43 Kpps	105.23 Kpps	Details

Ataque de reflexión/amplificación de SSDP

Affected Routers

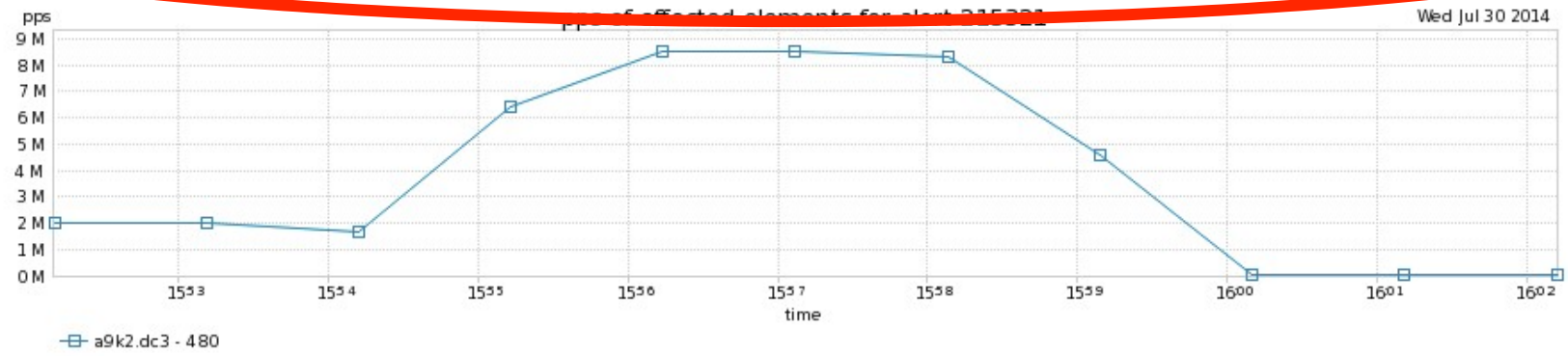
	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	50.00 Kpps	40.14 Gbps	20.25 Gbps	9.94 Mpps	4.7 Mpps	Details
Interface (SNMP 315) Bundle-Ether2.1013		-	1.20 Gbps	549.60 Mbps	287.47 Kpps	166.81 Kpp	
Interface (SNMP 344) Bundle-Ether100.2002		-	3.89 Mbps	2.15 Mbps	1.48 Kpps	757.14 pps	Details
Interface (SNMP 299) Bundle-Ether6453		-	10.62 Gbps	3.70 Gbps	965.25 Kpps	559.58 Kpps	Details
Interface (SNMP 478) Bundle-Ether44530		-	5.40 Mbps	5.22 Mbps	533.00 pps	505.56 pps	Details
Interface (SNMP 480) Bundle-Ether1299		-	22.46 Gbps	14.26 Gbps	8.52 Mpps	3.83 Mpps	Details
Interface (SNMP 569) Bundle-Ether3356		-	4.96 Gbps	1.81 Gbps	448.37 Kpps	295.68 Kpps	Details
Interface (SNMP 626) Bundle-Ether3.4090		-	2.11 Gbps	792.03 Mbps	191.38 Kpps	90.91 Kpps	Details
Router	High	50.00 Kpps	2.24 Gbps	934.88 Mbps	294.82 Kpps	178.77 Kpps	Details
Interface (SNMP 88) TenGigE0/0/0/17		-	2.22 Mbps	1.78 Mbps	200.00 pps	155.56 pps	Details
Interface (SNMP 274) TenGigE0/0/0/11.4080		-	2.49 Mbps	1.76 Mbps	233.00 pps	161.11 pps	Details
Interface (SNMP 361) Bundle-Ether44530		-	12.51 Mbps	5.46 Mbps	1.12 Kpps	891.44 pps	Details
Interface (SNMP 445) Bundle-Ether3.4080		-	2.09 Gbps	787.81 Mbps	189.22 Kpps	90.86 Kpps	Details
Interface (SNMP 470) TenGigE0/4/0/20.4		-	634.94 Mbps	298.68 Mbps	244.43 Kpps	105.23 Kpps	Details

Ataque de reflexión/amplificación de SSDP

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
215321	High 11,299.8% Of 90.0 Kpps	42.62 Gbps 3.86 Mpps	0:13 (Ended)	Wed, Jul 30 2014, 15:50:04	Incoming	UDP (Misuse)	[redacted]



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	50.00 kpps	40.14 G	20.25 G	9.94 M	4.79 M
Interface 480 Bundle-Ether1299 [redacted]		-	22.46 G	14.26 G	8.52 M	3.83 M

Ataque de reflexión/amplificación de SSDP

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
1.18 T	2.53 G	465.76	14.26 G	3.83 M

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	721.81 G	1.11 G	647.97	8.75 G	1.69 M	44.12	☑
27.192.0.0/11 ?	138.49 G	428.31 M	323.35	1.68 G	648.95 k	16.96	☑
117.0.0.0/9 ?	99.91 G	311.60 M	320.63	1.21 G	472.12 k	12.34	☑
218.0.0.0/9 ?	84.05 G	259.96 M	323.32	1.02 G	393.88 k	10.30	☑
180.96.0.0/11 ?	68.35 G	213.31 M	320.45	828.54 M	323.19 k	8.45	☑
27.128.0.0/9 ?	63.46 G	197.93 M	320.62	769.22 M	299.89 k	7.84	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1900	udp (17)	703.33 G	2.18 G	322.31	8.53 G	3.31 M	86.42	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	145.17 M	1.33 M	108.91	1.76 M	2.02 k	0.05	☐

Destination Ports

Ataque de reflexión/amplificación de SSDP

Summary

	Bytes	Packets	Bytes/Pkt	bps	pps
	1.18 T	2.53 G	465.76	14.26 G	3.83 M

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	721.81 G	1.11 G	647.97	8.75 G	1.69 M	44.12	☑
27.192.0.0/11 ?	138.49 G	428.31 M	323.35	1.68 G	648.95 k	16.96	☑
117.0.0.0/9 ?	99.91 G	311.60 M	320.63	1.21 G	472.12 k	12.34	☑
218.0.0.0/9 ?	84.05 G	259.96 M	323.32	1.02 G	393.88 k	10.30	☑
180.96.0.0/11 ?	68.35 G	213.31 M	320.45	828.54 M	323.19 k	8.45	☑
27.128.0.0/9 ?	63.46 G	197.93 M	320.62	769.22 M	299.89 k	7.84	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1900	udp (17)	703.33 G	2.18 G	322.31	8.53 G	3.31 M	86.42	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	145.17 M	1.33 M	108.91	1.76 M	2.02 k	0.05	☐

Destination Ports

Ataque de reflexión/amplificación de SSDP

Summary

	Bytes	Packets	Bytes/Pkt	bps	pps
	1.18 T	2.53 G	465.76	14.26 G	3.83 M

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	721.81 G	1.11 G	647.97	8.75 G	1.69 M	44.12	☑
27.192.0.0/11 ?	138.49 G	428.31 M	323.35	1.68 G	648.95 k	16.96	☑
117.0.0.0/9 ?	99.91 G	311.60 M	320.63	1.21 G	472.12 k	12.34	☑
218.0.0.0/9 ?	84.05 G	259.96 M	323.32	1.02 G	393.88 k	10.30	☑
180.96.0.0/11 ?	68.35 G	213.31 M	320.45	828.54 M	323.19 k	8.45	☑
27.128.0.0/9 ?	63.46 G	197.93 M	320.62	769.22 M	299.89 k	7.84	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1900	udp (17)	703.33 G	2.18 G	322.31	8.[illegible] G	3.31 M	86.42	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 [illegible]	514.87 k	13.46	☑
0 - 32767	udp (17)	145.17 M	1.33 M	108.91	1.76 M	2.02 k	0.05	☐

Destination Ports

Ataque de reflexión/amplificación de SSDP

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
300	udp (17)	703.57 G	2.18 G	322.31	8.53 G	3.31 M	86.45	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	29.05 M	21.00 k	1.38 k	352.14 k	31.82	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
Bundle-Ether1299	480	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
TenGigE0/7/0/20	143	793.91 G	2.25 G	353.08	9.62 G	3.41 M	89.05	☑
TenGigE0/0/0/10.409	705	359.31 G	261.05 M	1.38 k	4.36 G	395.53 k	10.34	☑
index:0	0	6.89 G	4.68 M	1.47 k	83.55 M	7.09 k	0.19	☐

Ataque de reflexión/amplificación de SSDP

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
300	udp (17)	703.57 G	2.18 G	322.31	8.53 G	3.31 M	86.45	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	29.05 M	21.00 k	1.38 k	352.14 k	31.82	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
Bundle-Ether1299	480	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
TenGigE0/7/0/20	143	793.91 G	2.25 G	353.08	9.62 G	3.41 M	89.05	☑
TenGigE0/0/0/10.409	705	359.31 G	261.05 M	1.38 k	4.36 G	395.53 k	10.34	☑
index:0	0	6.89 G	4.68 M	1.47 k	83.55 M	7.09 k	0.19	☐

¿Cuánto tráfico produce un ataque DDoS de 100 gb/s?

¿Cuánto tráfico falsificado produce un ataque DDoS de 100 gb/s?

- **DNS - Factor de amplificación 160:1**
  - **625mb/seg** de consultas DNS falsas para un ataque de **100gb/seg**
  - El mayor observado en 2014 - 104gb/seg, 125gb/seg reportado
- **ntp - factor de amplificación 1000:1**
  - **100mb/seg** de consultas ntp falsas para un ataque de **100gb/seg**
  - El mayor observado en 2014 - 325gb/seg, 450gb/seg reportado
- **chargen - 18:1 / 1000:1 factor de amplificación**
  - **100mb/seg - 5,5gb/seg** de consultas de carga falsas para un ataque de **100gb/seg**
  - El mayor observado en 2014 - 96gb/seg, 120gb/seg reportado
- **SNMP - Factor de amplificación 880:1 para un ataque optimizado**
  - **114 mb/s** de consultas SNMP falsas e iteradas para un ataque de **100 gb/s**
  - El mayor observado en 2014 - 18gb/seg, 60gb/seg reportado
- **SSDP - factor de amplificación 20:1 / 83:1**
  - **1,2gb/seg - 5gb/seg** de consultas SSDP falsas para un ataque de **100gb/seg**
  - El mayor observado en 2014: 131gb/seg.
- **Servicio de replicación de MS SQL, también conocido como SQL Slammer-on-Demand - Factor de amplificación 173:1 - 473:1**
  - **211mb/seg - 578mb/seg** de consultas MS SQL RS falsificadas para un ataque **de 100gb/seg**
  - El mayor observado en 2014 - N/A

Mitigación de la Reflección/Amplificación de Ataques DDoS

Lo que *no hay* que hacer

- ***No*** bloquee indiscriminadamente UDP/123 en sus redes.
- ***No*** bloquee indiscriminadamente UDP/53 en sus redes.
- ***No*** bloquee los paquetes UDP/53 de más de 512 bytes.
- ***No*** bloquee TCP/53 en sus redes.
- ***No*** bloquee indiscriminadamente UDP/161 en sus redes.
- ***No*** bloquee indiscriminadamente UDP/19 en sus redes.
- ***No*** bloquee indiscriminadamente UDP/1900 en sus redes.
- ***No*** bloquee indiscriminadamente los fragmentos en sus redes.
- ***No*** bloquee todo el ICMP en su networks! Al menos, permita el ICMP Tipo-3/Código-4, necesario para PMTU-D.

Si hace estas cosas, ***¡romperá Internet*** para sus clientes/usuarios!

No seas parte del problema!

- Despliegue de **antispoofing** en ***todos los*** bordes de la red.
  - **uRPF Loose-Mode/Feasible-Mode** en el borde de peering
  - **Modo estricto uRPF** en el borde de agregación del cliente
  - **ACLs** en el borde de agregación del cliente
  - **uRPF Strict-Mode** y/o **ACLs** en el borde de agregación del Centro de Datos de Internet (IDC)
  - **DHCP Snooping** (también funciona para direcciones estáticas) y **verificación de la fuente IP** en el borde de acceso de la LAN del IDC
  - **PACLs** y VACLs **en** el borde de acceso de la LAN de IDC
  - **Cable IP Source Verify**, etc. en el CMTS
  - **Otros** mecanismos DOCSIS y DSL
- Si adquiere la reputación de ser una red favorable a la suplantación de identidad, será **desviado/desviado** y/o **bloqueado**!

No seas parte del problema! (cont.)

- ***Escanear proactivamente*** y remediar los servicios abusivos ***en su red*** y en ***las redes de los clientes/usuarios***, incluyendo el bloqueo del tráfico hacia/desde los servicios abusivos si es necesario para lograr el cumplimiento.
- Compruebe en http://www.openntpproject.org si se han identificado servicios NTP abusivos en sus redes y/o redes de clientes/usuarios
- Compruebe http://www.openresolverproject.org para ver si se han identificado recursores DNS abiertos abusivos en su red o en las redes de clientes/usuarios.
- Los ***daños colaterales*** de estos ataques son generalizados: si hay servicios abusivos en sus redes o en las redes de clientes/usuarios***, sus clientes/usuarios experimentarán importantes cortes*** y problemas de rendimiento, y su servicio de asistencia técnica se encenderá.

Detección/Clasificación/Recuperación/Mitiga

- Utilizar **la telemetría de flujo** (NetFlow, cflowd/jflow, etc.) exportada desde
  todos los bordes de la red para la detección/clasificación/rastreo de ataques
  - -Muchas herramientas de código abierto disponibles, ¡no hay excusa para no empezar!
- Aplique **políticas de acceso a la red estándar** frente a los servidores/servicios mediante ACL sin estado en routers basados en hardware/conmutadores de capa 3.
- Asegúrese de que los servidores DNS recursivos **no sean consultables** desde la Internet pública, sólo desde sus clientes/usuarios.
- Asegúrese de que **SNMP está deshabilitado/bloqueado** en la infraestructura/servidores de cara al público.

Detección/Clasificación/Recuperación/Mitiga

- No permitir las **consultas NTP de nivel 6/-7** desde la Internet pública.
- Desactiva todos los **servicios innecesarios**, como Chargen.
- **Auditar periódicamente la** infraestructura de red y los servidores/servicios.

Detección/Clasificación/Recuperación/Mitigación

- Implantar técnicas de reacción/mitigación basadas en la infraestructura de la red, como **S/RTBH** y **flowspec**, en ***todos los*** bordes de la red.
- Despliegue sistemas inteligentes de mitigación de DDoS (IDMS) en centros de mitigación ubicados en puntos topológicamente apropiados dentro de sus redes para mitigar los ataques.
- Garantizar ***suficiente capacidad de mitigación y ancho de banda de desvío/reinyección*** - S/RTBH, flowspec, IDMS. Considerar los enlaces del centro de mitigación OOB desde los routers de borde para garantizar el ancho de banda de IDMS. "lavado".
- Las empresas/ASP deberían suscribirse a los servicios de mitigación de DDoS "**Clean Pipes**" de los ISP/MSSP.
- Los operadores de banda ancha de consumo deberían considerar la posibilidad de **establecer ACL mínimas por defecto** para limitar el impacto del abuso del servicio en las redes de los clientes.

Detección/Clasificación/Recuperación/Mitigación

- Utilice el **poder de la RFP** para especificar configuraciones seguras por defecto para los dispositivos PE y CPE, y verifíquelas mediante pruebas.
- **Saber a quién dirigirse** en sus pares/tránsitos para obtener ayuda.
- **Participar** en la comunidad global de seguridad operativa.

Detección/Clasificación/Recuperación/Mitigación

- Los ISPs deberían considerar el despliegue de mecanismos de **calidad de servicio (QoS)** en todos los bordes de la red para controlar el tráfico NTP no sincronizado a un nivel apropiado (por ejemplo, 1mb/seg).
  - Los paquetes NTP timesync tienen una longitud de 76 bytes (todos los tamaños son menos la trama de la capa 2)
  - Las respuestas de NTP monlist tienen una longitud de ~468 bytes
  - Las peticiones NTP monlist utilizadas en estos ataques tienen una longitud de 50, 60 y 234 bytes
  - **Opción 1** - vigilar todo el tráfico UDP/123 que no sea de 76 bytes (origen, destino o ambos) hasta 1mb/seg. Esto vigilará tanto el tráfico de ataque origen - reflector/amplificador como el tráfico reflector/amplificador - destino.
  - **Opción 2** - vigilar todo el tráfico UDP/123 de 400 bytes o más (origen) hasta 1mb/seg. Esto vigilará sólo el reflector/amplificador - el tráfico de destino
  - El tráfico NTP timesync no se verá afectado
  - Las funciones administrativas adicionales de NTP (poco utilizadas), como *ntptrace*, sólo se verán afectadas durante un ataque
- Las empresas/ASP sólo deben permitir consultas/respuestas NTP a/desde **servicios NTP específicos**, y no permitir el resto.

Escalar la capacidad de mitigación - 4tb/seg y más allá

- Sistema inteligente de mitigación de DDoS (IDMS) de mayor capacidad actualmente en el mercado: 40 GB/seg.
- 16-IDMS (límite CEF/ECMP) = 640gb/seg por cluster
- Se pueden emitir múltiples clusters
- Mayor número de IDMS por despliegue actualmente 100 = 4tb/seg de capacidad de mitigación por despliegue, 10 veces más que el mayor DDoS hasta la fecha.
- Despliegue de IDMS en centros de mitigación en los bordes - en/de los dispositivos de borde.
- Despliegue los IDMS en centros de mitigación regionales o centralizados con enlaces de desvío/reinyección OOB dedicados y de alta capacidad. El ancho de banda suficiente para la desviación/reinyección es fundamental.
- S/RTBH y flowspec aprovechan el hardware de los routers/conmutadores, cientos de mpps, . gb/segSe requiere

aprovechar .la infraestructura de red debido a la relación entre los volúmenes de ataque y las capacidades de los enlaces centrales y de peering.

Conclusión
.

Reflexión/Amplificación Resumen del ataque DDoS

- Los servicios abusivos están ampliamente mal implementados/mal configurados en Internet
- Grandes grupos de servidores/servicios abusivos
- Lagunas en el anti-spoofing en los bordes de la red
- Altos índices de amplificación
- Baja dificultad de ejecución
- Herramientas de ataque fácilmente disponibles
- Impacto extremadamente alto - "¡El cielo se está cayendo!
- Riesgo significativo para los objetivos potenciales y las redes intermedias/personas ajenas

Sobre el origen del tráfico falsificado

- NAT es feo, rompe cosas y no tiene ningún valor de seguridad inherente.
- Sin embargo, la prevalencia de la NAT en las redes de acceso de banda ancha ha tenido un efecto secundario beneficioso: el anti-spoofing (generalmente no se puede falsificar el tráfico desde detrás de una NAT, a menos que esté rota).
- Creemos que gran parte del tráfico falsificado que se utiliza para iniciar ataques DDoS de reflexión/amplificación se origina en servidores bajo el control de los atacantes en centros de datos de Internet (IDC) de alojamiento/co-localización/VPS/nube que no aplican la validación de la dirección de origen.
- Los servidores pueden estar comprometidos; pueden ser VPS alquilados por atacantes; pueden estar alojados por proveedores "a prueba de balas".
- Las herramientas de recopilación/análisis de telemetría de flujos realizan un rastreo automático del tráfico falsificado hasta los puntos de entrada de la red, pero sólo dentro del propio ámbito de control administrativo.

¿Qué hay que hacer?

- Iniciar un proyecto para alquilar instancias de shell/VPS en todo el mundo, ejecutar código del tipo del Proyecto Spoofer en las instancias de VPS, compilar informes de IDCs/hosters/co-localizadores que permiten el spoofing. Por lo menos, un punto de partida.
- Discutir la posibilidad de incluir funcionalidades del tipo del Proyecto Spoofer en los sistemas operativos con los vendedores/organizaciones pertinentes (Microsoft, Apple, Google, distros de Linux, distros de *BSD, vendedores de consolas, Cisco, Juniper, Linksys, Asus, etc.).
- Mecanismo de aprendizaje para la funcionalidad del tipo IP Source Guard o pACL/vACL habilitado por defecto en los puertos de conmutadores de capa 2 configurados como puertos de acceso - vendedores de infraestructura de red. La capa de acceso IDC es un dominio relativamente restringido con un menor alcance de resultados indeseables y una mayor probabilidad de éxito.
- ¿Mecanismos de autoaprovisionamiento de direcciones de origen de la SDN?
- Mejorar la clasificación del tráfico falsificado, las capacidades de rastreo cooperativo entre operadores - proveedores de herramientas de recopilación/análisis de telemetría de flujos.
- Trabajar con las compañías de seguros para ayudarles a entender los riesgos no asegurados, desarrollar capacidades de auditoría.

¿Estamos condenados?

- La No! implementación de herramientas/técnicas/BCPs No! existentes y bien conocidas da lugar a una postura de seguridad muy mejorada con resultados medibles.
- La evolución de las defensas contra estos ataques demuestra que es posible un cambio positivo: las organizaciones objetivo y los ISP/MSSP defensores han modificado las arquitecturas, las técnicas de mitigación, los procesos y los procedimientos para mitigar con éxito estos ataques.
- Las capacidades de mitigación se están ampliando para satisfacer y superar los volúmenes de ataques: la arquitectura de despliegue, el ancho de banda de desviación/reinyección y el aprovechamiento de la infraestructura de red son fundamentales.
- La automatización es una buena cosa, pero no sustituye a una arquitectura resistente, una planificación perspicaz y un personal de operaciones inteligente, que son más importantes ahora que nunca.

Debate

Esta presentación - http://bit.ly/1lHksUH

Un agradecimiento especial a Gary Sockrider y Ben Fischer de Arbor Networks por su contribución a esta presentación.

Gracias.

Roland Dobbins < rdobbins@arbor.net>
Analista senior de ASERT