Marco de gestión de la seguridad bilateral (también conocido como peering DDoS)

CenturyLink y AT&T

Nimrod Levy, Don Smith, John Schiel

nl7942@att.com, donald.smith@Centurylink.com , John.Schiel@Centurylink.com

LEXICO

Flowspec Inter-ISP

- Anuncios de Flowspec iniciados por un peer DDoS para dejar caer el tráfico de ataque hacia una ip víctima

Tráfico no deseado

- Tráfico a filtrar por un ISP para el peering DDoS de

otro ISP

- Un ISP está dejando caer "tráfico no deseado" por otro

Peer

- Pares sin liquidación

ANTECEDENTES, SUPUESTOS Y CONTEXTO

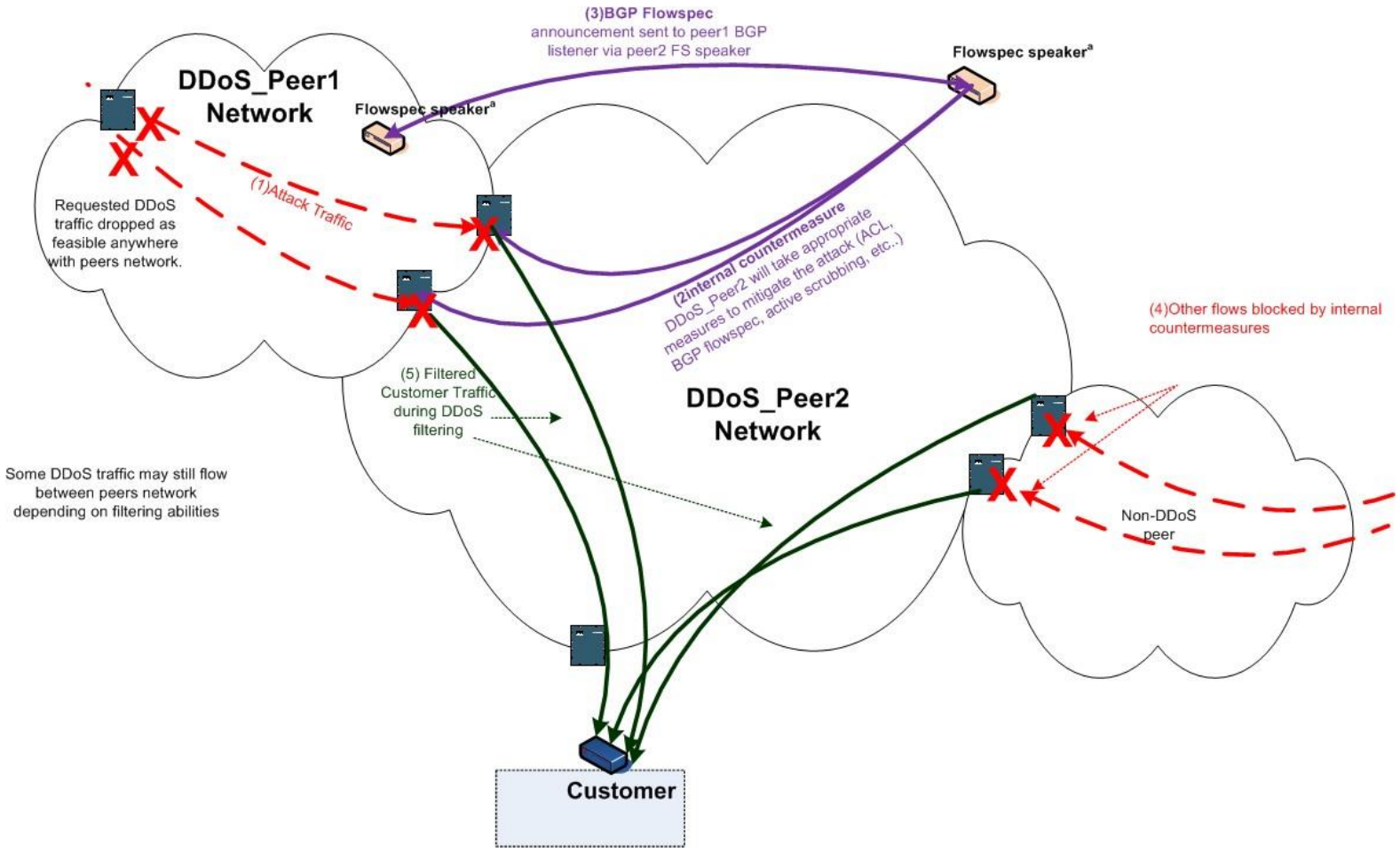
- Proporciona un proceso para que las redes pares intercambien solicitudes de filtrado
- Entre redes paritarias

- Una relación/entorno de beneficios recíprocos
- Institucional, no personal -> enfoque coherente

RAZONES PARA INICIAR EL ACERCAMIENTO A

- Impacto significativo en el cliente/víctima o en la infraestructura de la red solicitante
- Importante beneficio para la red notificada
- Transmitir las recomendaciones de higiene de la red
- Gestión de las vulnerabilidades
- Requisito previo: La red solicitante ha implementado mitigaciones razonables en su propia red

Diagrama de pares DDoS



SOLICITUDES : INICIAR, AUTENTIFICAR, VERIFICAR

- Debe tener los conceptos básicos de la AAA y la CIA.
- No sólo se requiere autentificación, autorización y contabilidad
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Métodos de filtrado seguro de solicitudes
  - Anuncios de rutas BGP / Flowspec inter-ISP
  - Llamar utilizando puntos de contacto preestablecidos
  - EMAIL a un alias común NOC/SOC
  - Sistema de tickets
  - Otros (TBD en marcos individuales)

TIPOS/ACCIONES ADMITIDAS (POR PARES)

- "estándar 5-tupla" + ICMP
- TIPOS disponibles

—	1: Prefijo de destino	2 : Prefijo de origen	3 : Protocolo	IP
- 4: Tipo de puerto	5: Puerto de destino	6: Puerto de origen		
- 7: Tipo de ICMP	8: Código ICMP	9: Banderas TCP		
- 10: Paquete LEN	11: DSCP	12: Fragmento		

- Tipos iniciales 1,3,5,6,7,8.
- Acciones permitidas -> abandonar
- ¿Justificación?

REGLAS PARA LOS ANUNCIOS DE RUTAS

- Max-prefijo N, alerta para el % de N, desmontaje en N+1
- Coherencia con los anuncios redundantes
- La duración es indefinida -> el prefijo máximo se retira entonces añade
- Acción inicial soltar paquetes
- Utilizar BGPv4 para rutas de flujo IPv4 e IPv6
- NO_EXPORT, límite de longitud /25 .../32
- Una comunidad coherente para este fin

RESPUESTA DE LA RED NOTIFICADA

- Implementar el bloqueo en cualquier punto razonable entre pares.
- Considerar la aplicación de prácticas de higiene en la red
- Agradecimiento
  - Recibimos su solicitud
  - Hicimos algo/en algún lugar
  - Bucle de retroalimentación

OTRAS CONSIDERACIONES

- Solicitudes retiradas/canceladas por el par solicitante
- Limitado a los eventos significativos
- Peer no tiene ninguna obligación, puede terminar la acción en cualquier momento a su discreción
- Ambas redes deben evaluar los impactos colaterales
- Implementar con los compañeros sobre una base bilateral

BENEFICIOS DE LA PILOTO/PRUEBA DE CONCEPTO

- Amplía la capacidad de los ISP para resistir grandes ataques DDoS
- La respuesta a los DDoS es más eficiente:
  - Relación institucional no personal
  - Una relación de confianza preestablecida/autentificada
  - Procesos prenegociados y predefinidos
  - Solicitudes documentadas, elementos de datos específicos
- Ventaja adicional de no llevar tráfico no deseado

PROBLEMAS/PREOCUP

- Legal/Política pública/Reglamentación
- Cuestiones de confidencialidad
- Informar

MATERIAL DE

- BCP 38 http://www.bcp38.info/index.php/Main_Page
- BCP 84 https://tools.ietf.org/html/bcp84
- UTRS http://www.team-cymru.org/UTRS/index.html
- Comunidad DBHF https://tools.ietf.org/html/rfc7999
- Flowspec
  - https://tools.ietf.org/html/rfc5575
  - https://www.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf