

Cadre de gestion de la sécurité bilatérale (a.k.a. DDoS peering)

CenturyLink et AT&T

Nimrod Levy, Don Smith, John Schiel

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

LEXICON

Inter-ISP Flowspec

- Annonces de flux initiées par un pair DDoS pour interrompre le trafic d'attaque vers un ip victime.


Trafic indésirable

- Trafic à filtrer par un ISP pour un autre ISP **Peering**

DDoS

- Un ISP laisse tomber le "trafic indésirable" pour un autre **pair**.
- Pair sans règlement

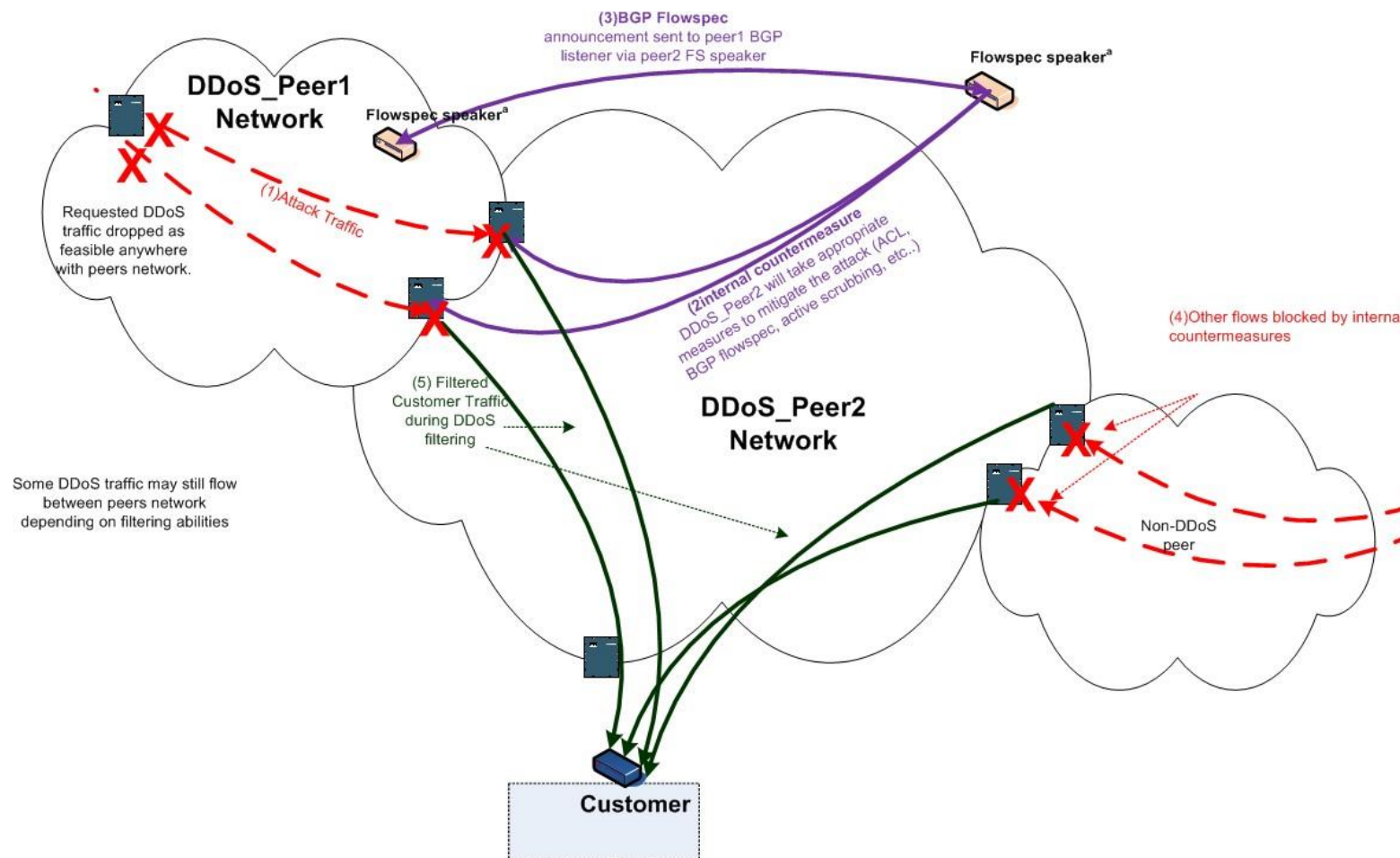
HISTORIQUE, HYPOTHÈSES ET CONTEXTE

- Fournit un processus permettant aux réseaux homologues d'échanger des demandes de filtrage.
- Entre les réseaux d'échange de trafic 
- Une relation/un environnement pour des bénéfices réciproques
- Institutionnel, pas personnel -> approche cohérente

LES RAISONS D'ENTREPRENDRE DES ACTIONS DE

- Impact important sur le client/la victime ou l'infrastructure du réseau demandeur.
- Un avantage significatif pour le réseau notifié
- Transmettre les recommandations d'hygiène du réseau
- Gestion des vulnérabilités
- Pré-requis : Le réseau demandeur a mis en place des mesures d'atténuation raisonnables sur son propre réseau.

Diagramme d'échange de trafic DDoS



DEMANDES : INITIER, AUTHENTIFIER, VÉRIFIER

- Doit avoir les concepts de base de l'AAA et de la CIA.
- Pas seulement Authentifié, Autorisé et Comptabilité requis
 - Confidentialité
 - Intégrité
 - Disponibilité
- Méthodes de filtrage sécurisé des demandes
 - Annonces de routes BGP / Flowspec inter-ISP
 - Appeler en utilisant des points de contact préétablis
 - EMAIL vers un alias commun CNO/SOC
 - Système de billetterie
 - Autres (à déterminer dans les cadres individuels)

TYPES/ACTIONS SUPPORTÉS (PAR PAIR)

- "5-tuple standard" + ICMP

- TYPES disponibles

—	1 : Dest Prefix2	: SrcPrefix3	: Protocole	IP
- 4 : Type de port	5 : Dest port	6 : Port Src		
- 7 : Type ICMP	8 : Code ICMP	9 : drapeaux TCP		
- 10 : LEN du paquet	11 : DSCP	12 : Fragment		

- Types initiaux 1,3,5,6,7,8.
- Actions autorisées -> abandonner
- La justification ?

RÈGLES POUR LES ANNONCES DE ROUTE

- Préfixe maximal N, alerte pour % de N, arrêt à N+1
- Cohérence avec les annonces redondantes
- La durée est indéfinie -> Préfixe max retirer puis ajouter
- Action initiale : abandon des paquets
- Utiliser BGPv4 pour les routes de flux IPv4 et IPv6
- NO_EXPORT, longueur limite /25 .../32
- Communauté cohérente à cet effet

RÉPONSE DU RÉSEAU NOTIFIÉ

- Mettre en œuvre le blocage à tout point raisonnable entre les pairs.
- Envisager la mise en œuvre d'une pratique d'hygiène du réseau
- Remerciements
 - Nous avons reçu votre demande
 - Nous avons fait quelque chose/quelque chose
 - Boucle de rétroaction

AUTRES CONSIDÉRATIONS

- Demandes retirées/annulées par le pair demandeur
- Limité aux événements significatifs
- Peer n'a aucune obligation, peut mettre fin à l'action à tout moment, à sa discrétion.
- Les deux réseaux doivent évaluer les impacts collatéraux
- Mise en œuvre avec les pairs sur une base bilatérale

LES AVANTAGES PILOTE/PREUVE DE CONCEPT

- Renforce la capacité des FAI à résister aux attaques DDoS de grande envergure
- Une réponse DDoS plus efficace :
 - Relation institutionnelle et non personnelle
 - Une relation de confiance préétablie/authentifiée
 - Processus pré-négociés et prédéfinis
 - Demandes documentées, éléments de données spécifiques
- Avantage supplémentaire de ne pas transporter de trafic indésirable

PROBLÈMES/PRÉOCCU

- Juridique/Politique publique/Réglementation
- Problèmes de confidentialité
- Reporting

MATÉRIEL 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>
- Communauté 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

MATÉRIEL DE