GRNET(Greek Research and Technology Network) FireCircle

ギリシャの広域ファイヤーウォールサービスのお話

Shishio Tsuchiya

shtsuchi@cisco.com

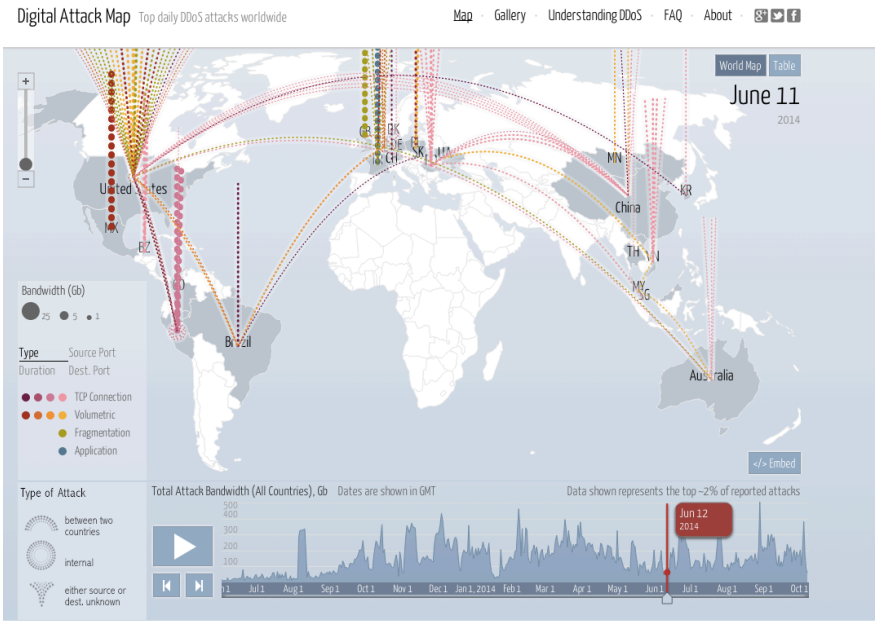
この話は

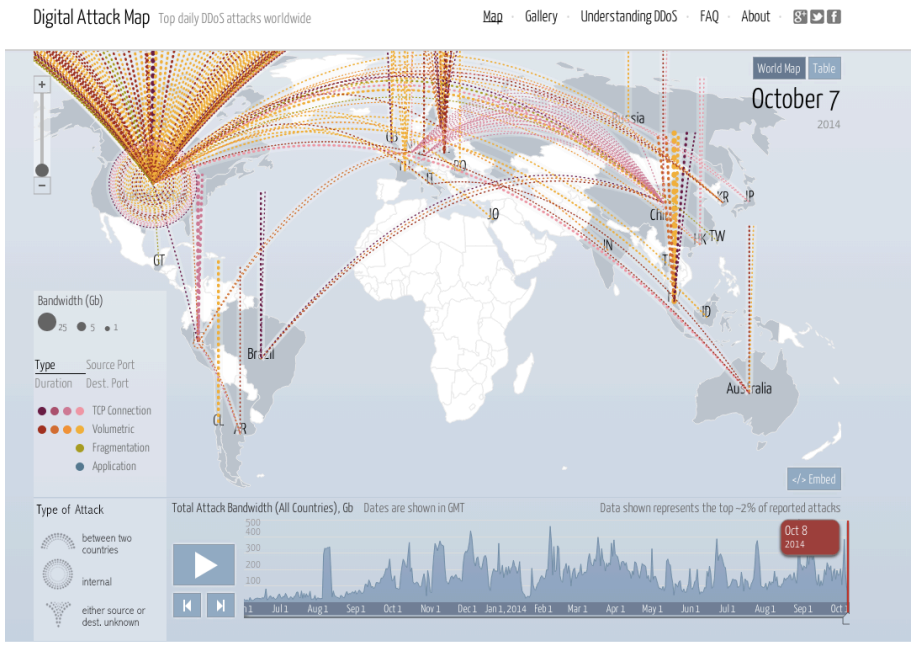
- TERENA Networking Conference (TNC) 2012で発表されたGRNETのお話です。
- BGP Flowspecの実装例を探してた所、見つけて面白そうだったのでシェアしてみます。

Agenda

- JANOG35のおさらい
- 海外の事例とGRNET

DDOSトラフィックは絶えず変化していく





http://www.digitalattackmap.com/

Atlas DDOSトレンドレポート

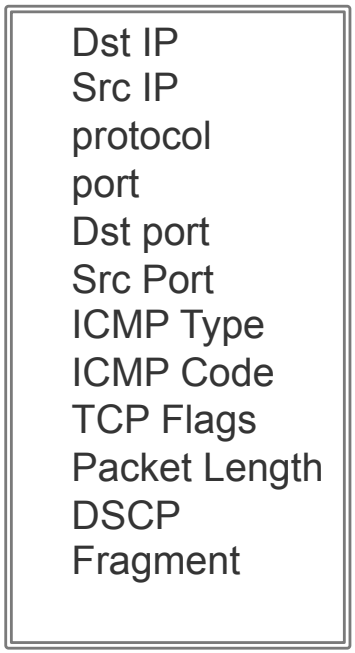
- DDOSボリューム(平均)
  - 日本 Q2:491.63Mbps Q3:365.8Mbps
  - アジア Q2:530.5Mbps Q3:588.74Mbps
  - 世界 Q2:759.83Mbps Q3:858.98Mbps
- NTPアンプ攻撃の傾向 (平均量)
  - 日本 Q2:3.22Gbps Q3:281.76Mbps☺
  - アジア Q2:2.57Gbps Q3:2.70Gbps
- アタック時間
  - 92%のDDOSは1時間以内に止まる
  - JAPAN:92%が1時間以内
    (平均時間は3時間21分)
  - アジア: 94.1%が1時間以内 平均31分
  - 5分お試し、1時間4＄などのサービスがある

- 次はなんだ☹
  - NTPアンプ攻撃は増大する事ができる
  - 攻撃者は次のプロトコルを探してる
  - SSDP(1900) が増加してる

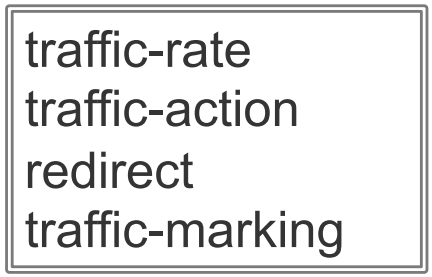
Services	UDP Source Port	Q3 Maximum DDOS Volume	Q3 Average DDOS Volume
SNMP	161	3.75Gbps	769.1Mbps
Chargen	19	21.26Gbps	1.12Gbps
DNS	53	43.45Gbps	1.31Gbps
SSDP	1900	51Gbps	5.11Gbps

http://www.janog.gr.jp/meeting/janog35/files/2014/2077/3840/janog35-bgpfs-agatsuma-1.pdf

BGP Flowspec(RFC5575)+draft-ietf-idr-flow-spec-v6



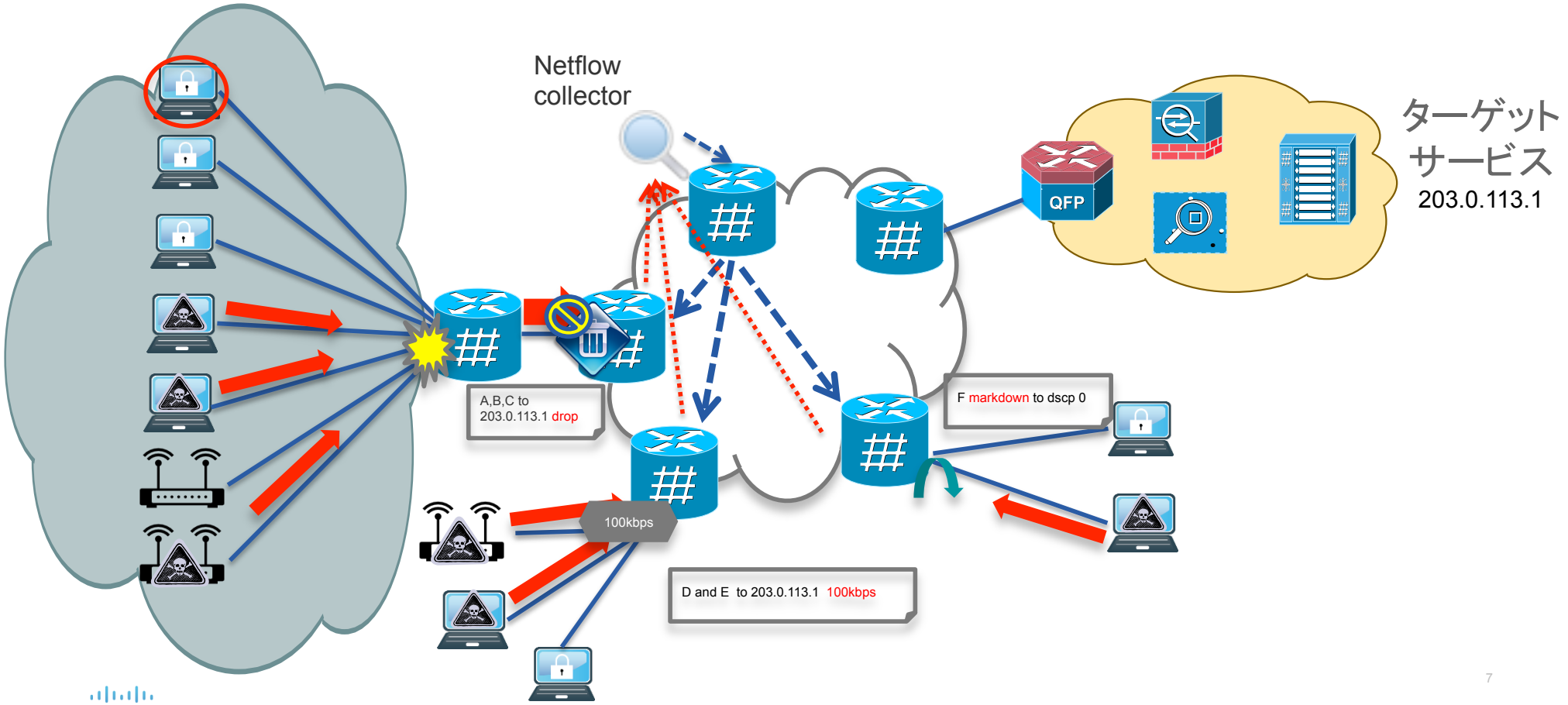
Flow Type



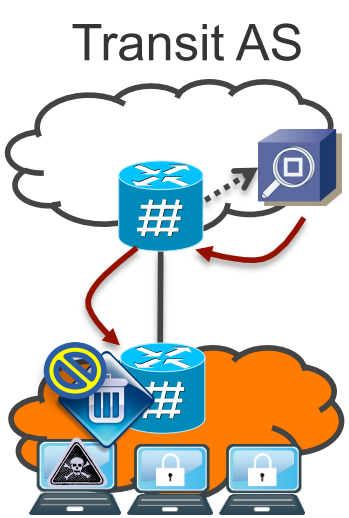
Action Rule

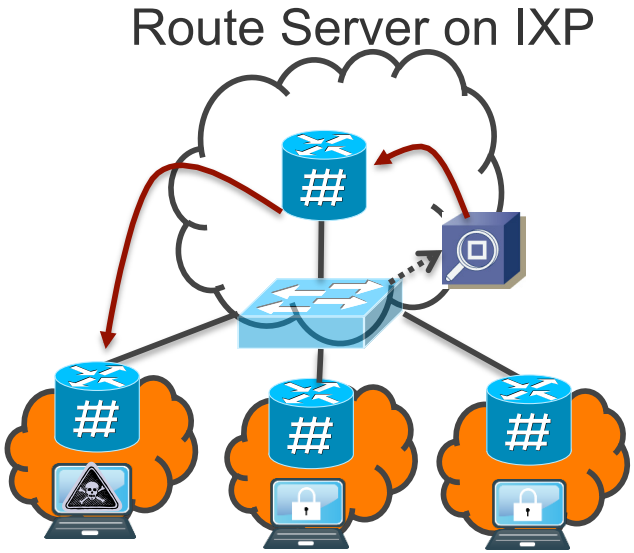
```
+-------------------------------------------------------+
|            AFI(2 octets)  1 and 2                     |
+-------------------------------------------------------+
|          SAFI (1 octet) 133 and 134                   |
+-------------------------------------------------------+
| Length of Next Hop Network Address (1 octet)          |
+-------------------------------------------------------+
| Network Address of Next Hop (variable)                |
+-------------------------------------------------------+
| Reserved (1 octet)                                    |
+-------------------------------------------------------+
| Network Layer Reachability Information (variable)     |
+-------------------------------------------------------+
```

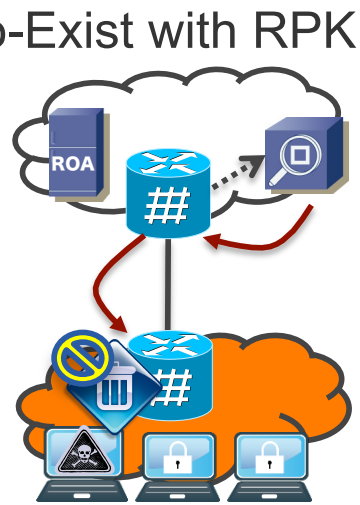
BGP Flowspec(RFC5575)



こんな質問ありました







- eBGPで使える？

  Transit ASから下位にコントロールして欲しい

- IXのルートサーバーから配信とか出来ない？
- RPKIと上手く連携できる？

Agenda

- JANOG35のおさらい
- 海外の事例とGRNET

Time Warner Telecom (TWTC) NANOG38 2006 Deployment Experience With BGP Flow Specification

https://www.nanog.org/meetings/nanog38/presentations/labovitz-bgp-flowsp

- DDOSの問題
  - 大きく、頻繁に顧客まで影響する
  - 顧客だけでは無くインフラも危険
  - 対策の為の運用コストが莫大
- DDoS解析
  - BOTNETやScript Kiddiesにより大きなDDOSが作られている
  - TCP Synフラッドは1Mbps以上
  - UDPフラグメント
  - APNIC（中国）からのアタックが大きい。グレートファイアーウォールのおかげでトラックしずらい
- RRからPeerとTransiのルータにFlowspecを使用
- クリーニン用のVRFを作り、Mitigation実施
- 出来なかったもの
  - マルチベンダーサポート（Juniper/Arborで構築）
  - インターAS
  - DSCP識別

Neo Telecoms FRNOG18 2011 Flowspec

http://media.frnog.org/FRnOG_18/FRnOG_18-6.pdf

- RTBH/PBRとFlowspec比較
  - RTBH(Remote Triggered Black Hole)

    WebsiteはDDOS攻撃から防御できる、でもトラフィックが・・・・来ない
  - PBR(Policy Based Routing)

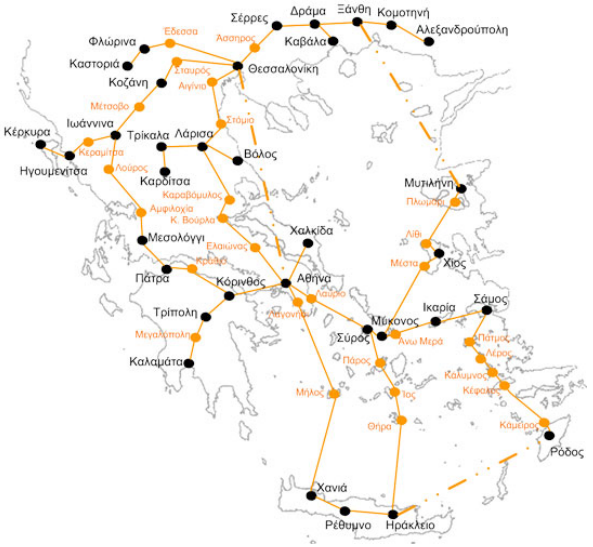
    ハードウェアでトラフィックコントロールできる

    どうやって、DDOSを検知し、ポリシーを適用したり、削除したりするか？
  - Flowspec

    PBRを動的で全般的に広告する 。新しい通信手段は必要無い
- AS内のtransitのルータで展開した

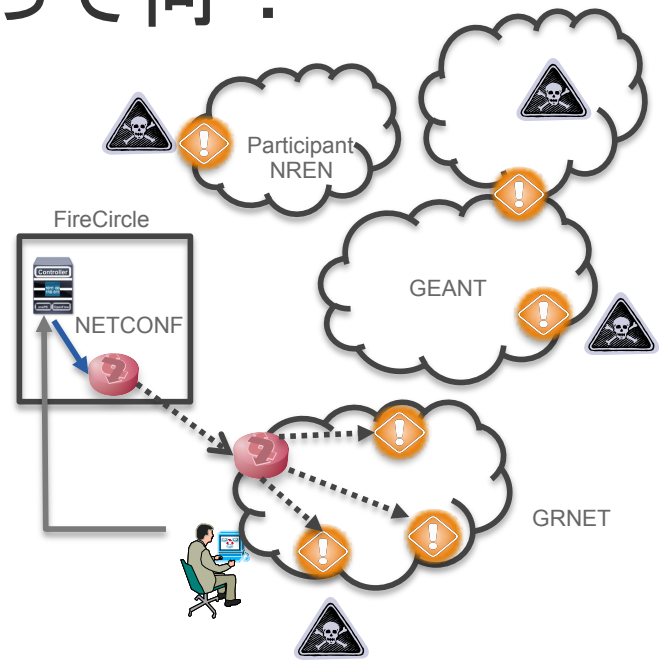
  eBGPで適用したかったが、顧客申告を信じられない。eBGPの所でFlowを有効にしたくないなどの理由で見送った
- 次の展開
  - IPv6/VPNv6サポート
  - トラフィックモニター
  - ベンダーの追加（この時点ではJuniperとAlcatelだけだった）

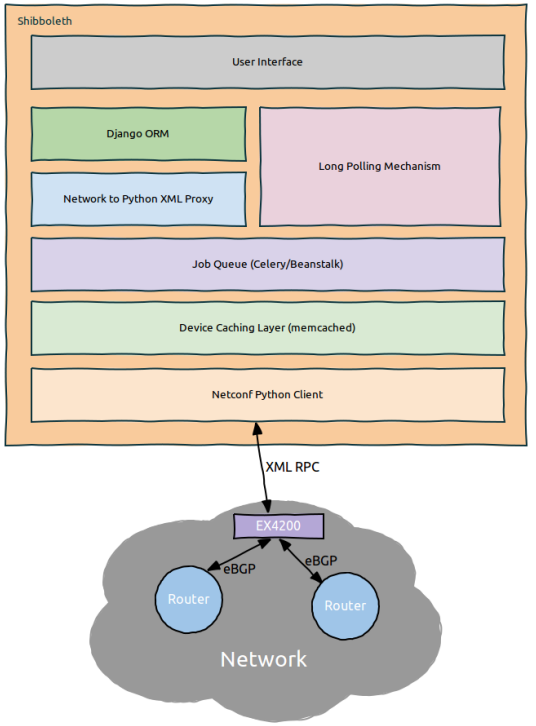
GRNETとは？



- Greek Research and Technology Network
- ギリシャのLIRとして活動 1995年以降
- GR-IXも運用
- GRNETは教育機関などにインターネットアクセスを提供
  - 27の大学・15の工科大学・33の研究機関・12673の学校(GEANT)

FireCircleって何？





- GRNETの客がWebでウイザート形式でFirewallルールを設定
- NETCONFでBGP Flowspecルータに設定
- BGP FlowspecルータはGRNET内のルータにアドバタイズ
- 各ルータはPBRでフローベースでフィルタリングもしくはレートリミット

Firewall On demand

- オープンソースです。
- EX4200（Juniper）をNETCONFでXML設定しちゃいます
- ここにあるよ
  https://fod.grnet.gr/

話しあいたい事

- eBGPでのFlowspecルール
  draft-ietf-idr-bgp-flowspec-oid
- YANGモデルって重要よ。
- 誰がルールアドバタイズしたら信じられる？
- こんなサービス出来るもん？？どこで？ISP間ならオッケー？客からの申請でオッケー？

Flowspec Validation process

下記の様な条件を満たさないとFlowspecとしてエントリーされない

Flowspecのoriginatorはその宛先プレフィックスのユニキャストルートのoriginatorと合致

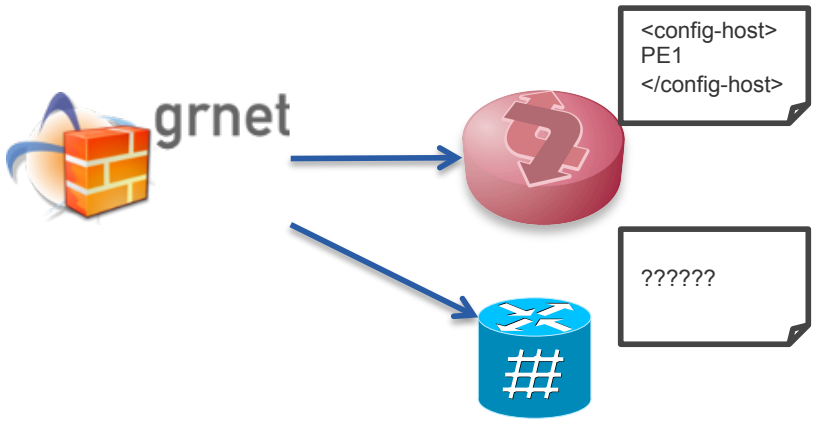
FlowspecのAS_PATHとAS4_PATHアトリビュートが空

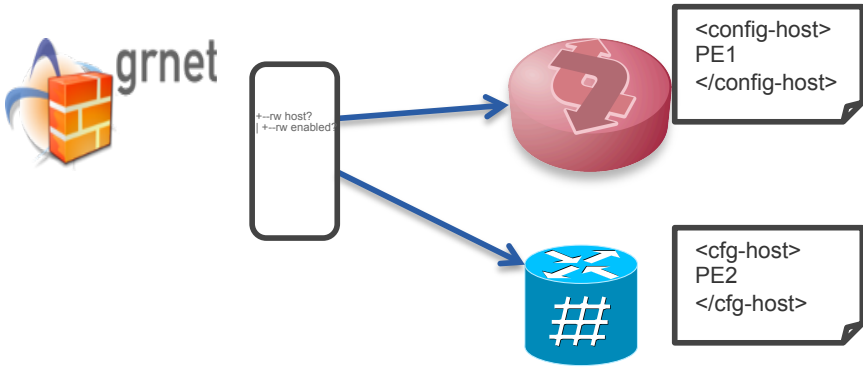
FlowspecのAS_PATH/AS4_PATHアトリビュートはAS_SET/AS_SEQUENCEを含まない

eBGPでは無効にする

```
router bgp 100
  neighbor x.x.x.x
   address-family ipv4/6 flowspec
    validation disable
```

YANGモデル





- NETCONF/XMLは標準的ではあるが、コンフィグ自体は各自が実装している
- 依存しない設計モデルが必要


CISCO
TOMORROW starts here.