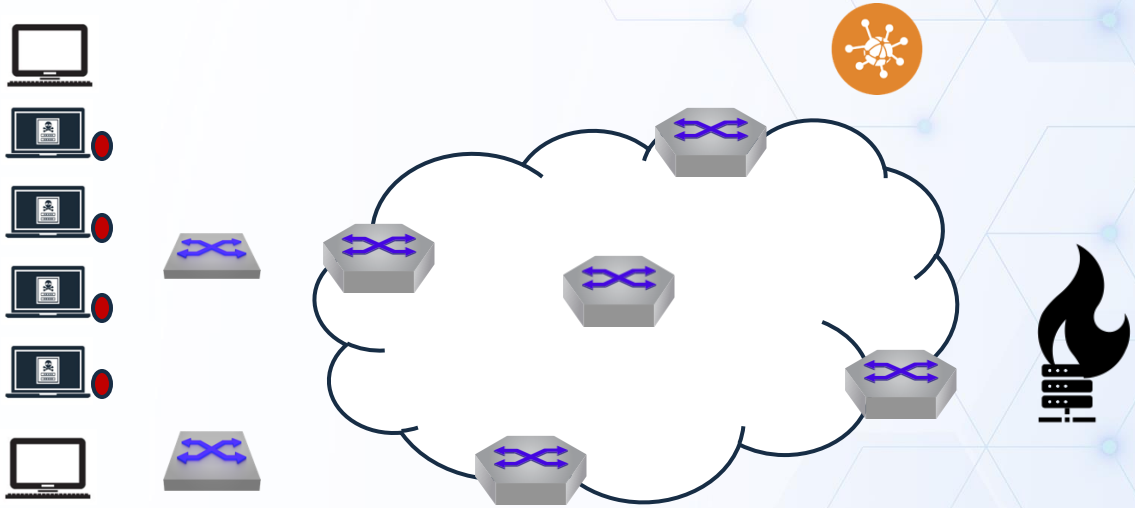
ARISTA

DDOS Protection by L2 switch

Shishio Tsuchiya

shtsuchi@arista.com

DDOS変化し続けている



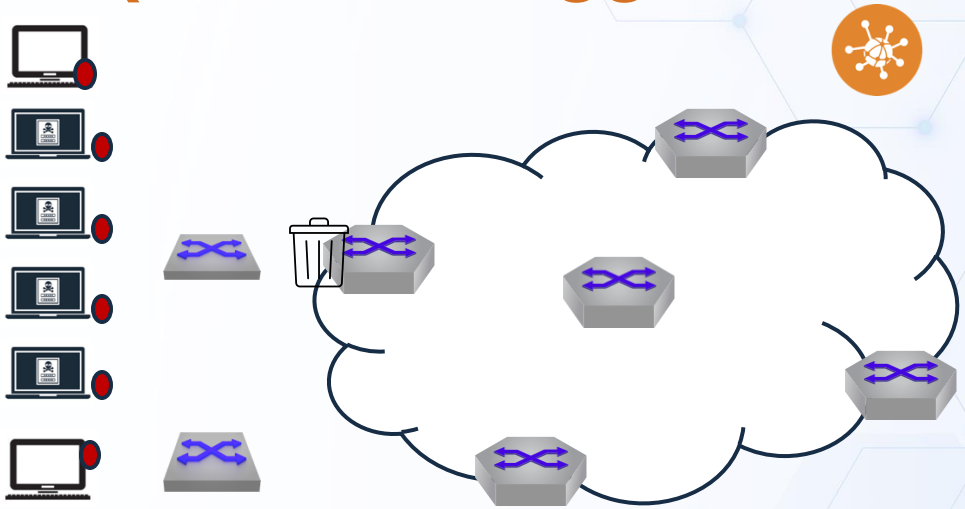
- DDOSはいつも変化してるし、そのトラフィックボリュームは莫大なものに
  - 2024年第4四半期、記録的な5.6TbpsのDDoS攻撃およびグローバルなDDoSの傾向
- サービスプロバイダーのネットワークではどうやってDDOSから防御してるのか？
- RTBH(Remote Triggered Black Hole)がISPでもっとも 使われてる技術といえる

 Copyright © Arista 2025. All rights reserved.

Confidential.

ARISTA

RTBH(Remote Triggered Black Hole)



```
route-map RTBH permit 10
   match tag 666
   set ip next-hop 198.51.100.66
   set origin igp
   set community no-export
!
ip route 198.51.100.18/32 Null0 tag 666
!
```

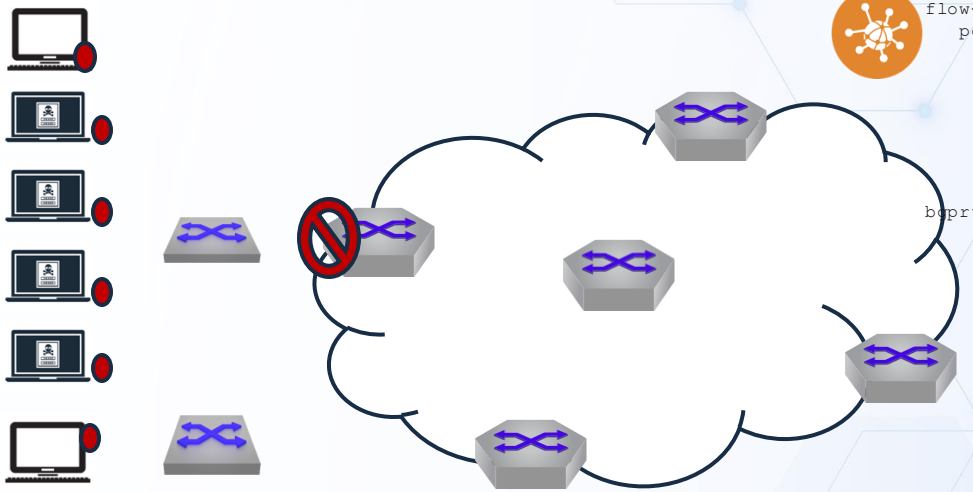
- RTBHはアタックされてるホストを防御する事が出来る
- しかしDDOSでも無いサービストラフィックにも悪影響を与えてしまう

 Copyright © Arista 2025. All rights reserved.

Confidential.

ARISTA

BGP Flowspec



```
bgprtr1(config)#flow-spec
bgprtr1(config-flow-spec)#policies
bgprtr1(config-flow-spec-policies)#show active
flow-spec
   policies
      policy p1
         match m1 ipv4
            destination prefix 10.0.0.0/24
            protocol tcp source port telnet destination port telnet
            !
            actions
               drop
bgprtr1(config-flow-spec-policies)#
```

- BGP Flowspecはフローとアクションを定義できる
- DDOSトラフィックフローに特定して防御する事が出来、通常のトラフィックに影響を与えない

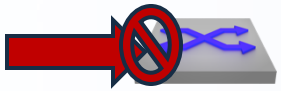
 Copyright © Arista 2025. All rights reserved.

Confidential.

ARISTA

DDOSとIP ACLを再考してみる

- DDOSは IPv4 またはIPv6、MACや他のレイヤー2プロトコルでは無い
- 最近のレイヤー2スイッチはレイヤー2のスイッチングポートにレイヤー3のルーティングポートと同様にL3/L4 ACLを設定する事ができる
- それなら・・・L2ポートにおけるflowspecは役立つかもしれない



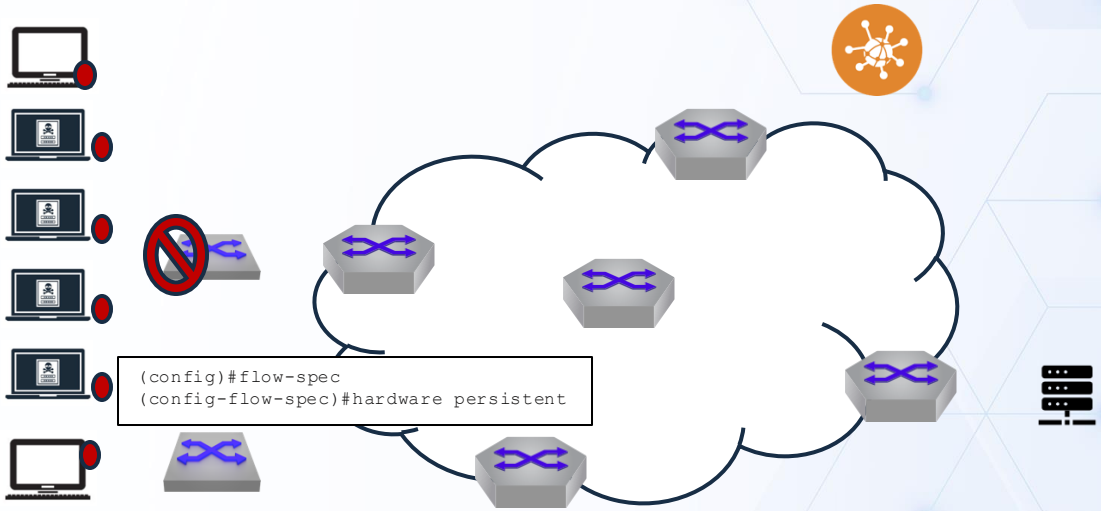
 Copyright © Arista 2025. All rights reserved.

Confidential.

ARISTA

BGP Flowspec on L2 Port

https://www.arista.com/en/support/toi/eos-4-23-2f/14437-bgp-flowspec#w2wwqm1viizn



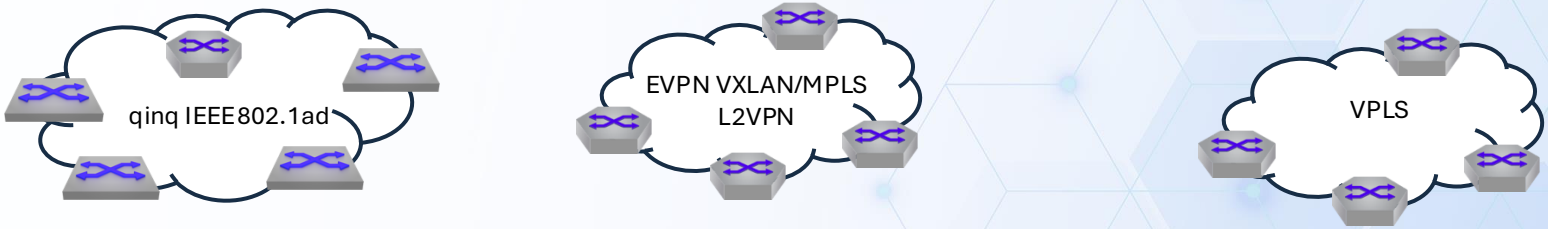
- 非常に少しの拡張ではあるが、サービスプロバイダーや広域イーサネットサービスに意義のある拡張をした
- BGPをレイヤー2スイッチのノースバンドのACLコンフィグオーケストレーターとして使える
- それはVPLSやEVPN L2VPNのネットワークエッジでも使える

 Copyright © Arista 2025. All rights reserved.

Confidential.

ARISTA

L2ポートへのFlowspecの有効性



- ISPの集約スイッチだけではなく、QinQやEVPN/VXLAN,EVPN/MPLSやVPLS/MPLSの広域イーサネットサービスでも使う事ができる

 Copyright © Arista 2025. All rights reserved.

Confidential.

ARISTA

ARISTA

Thank You

www.arista.com