Enhancing DDoS protection

TAYLOR HARRIS
SECURITY ENGINEER

Overview

- DDoS Evolution
- Typical Reactive/Proactive Mitigation
- Challenges and Obstacles
- BGP Flowspec
- Automated Flowspec Mitigation

DDoS Evolution

- As always, DDoS is on the rise
- >90% of attacks target residential*
- Schools, Banks, Government, and Financial Institutions are the next biggest targets
- Traffic is typically sourced from outside the U.S.
- Attacks are larger and more complex
- Emergence of free DDoS services

*MSO specific data

Typical Reactive DDoS Prevention

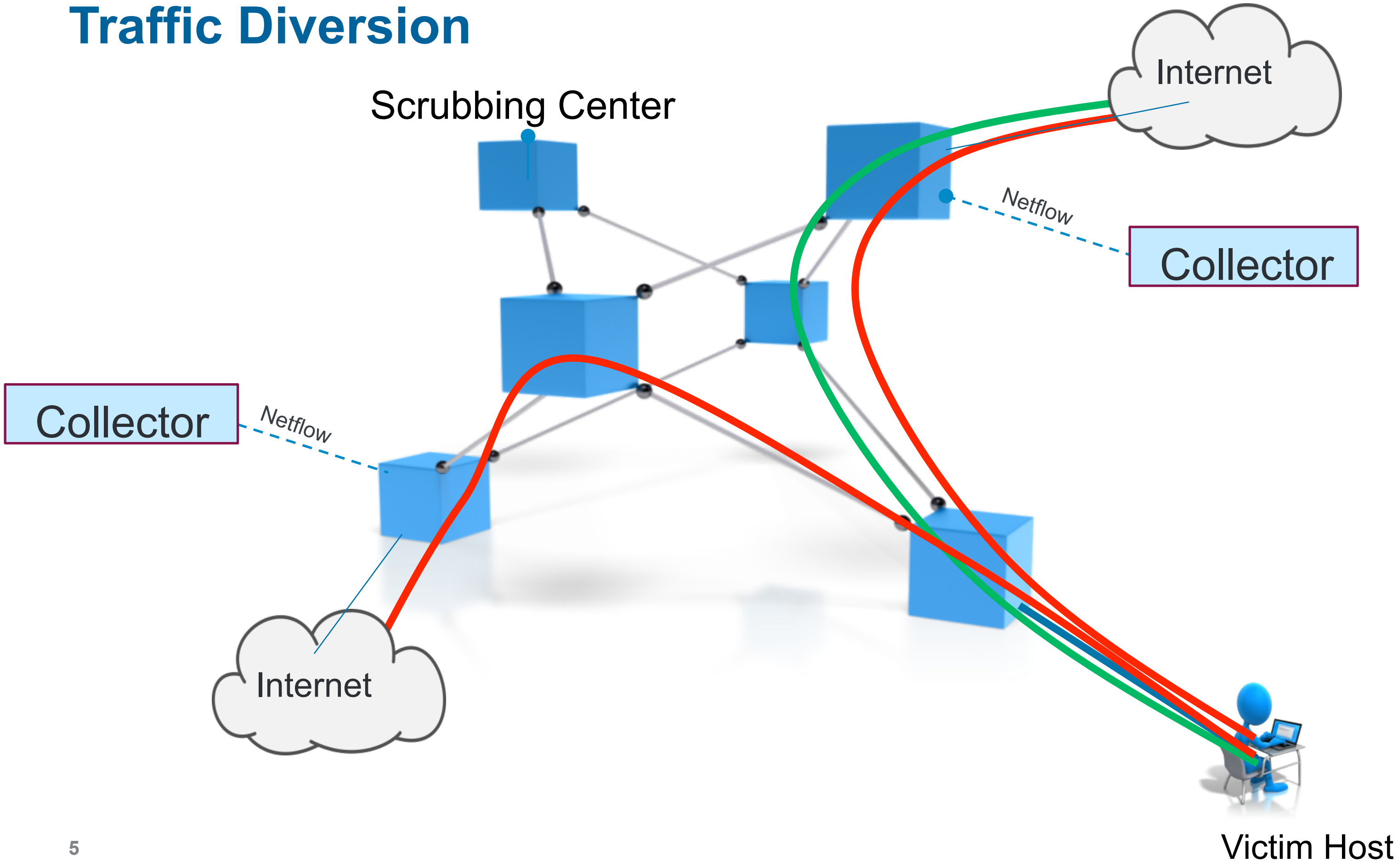
IN-LINE $OLUTION

- Costly
- Expensive
  - Also costly and expensive

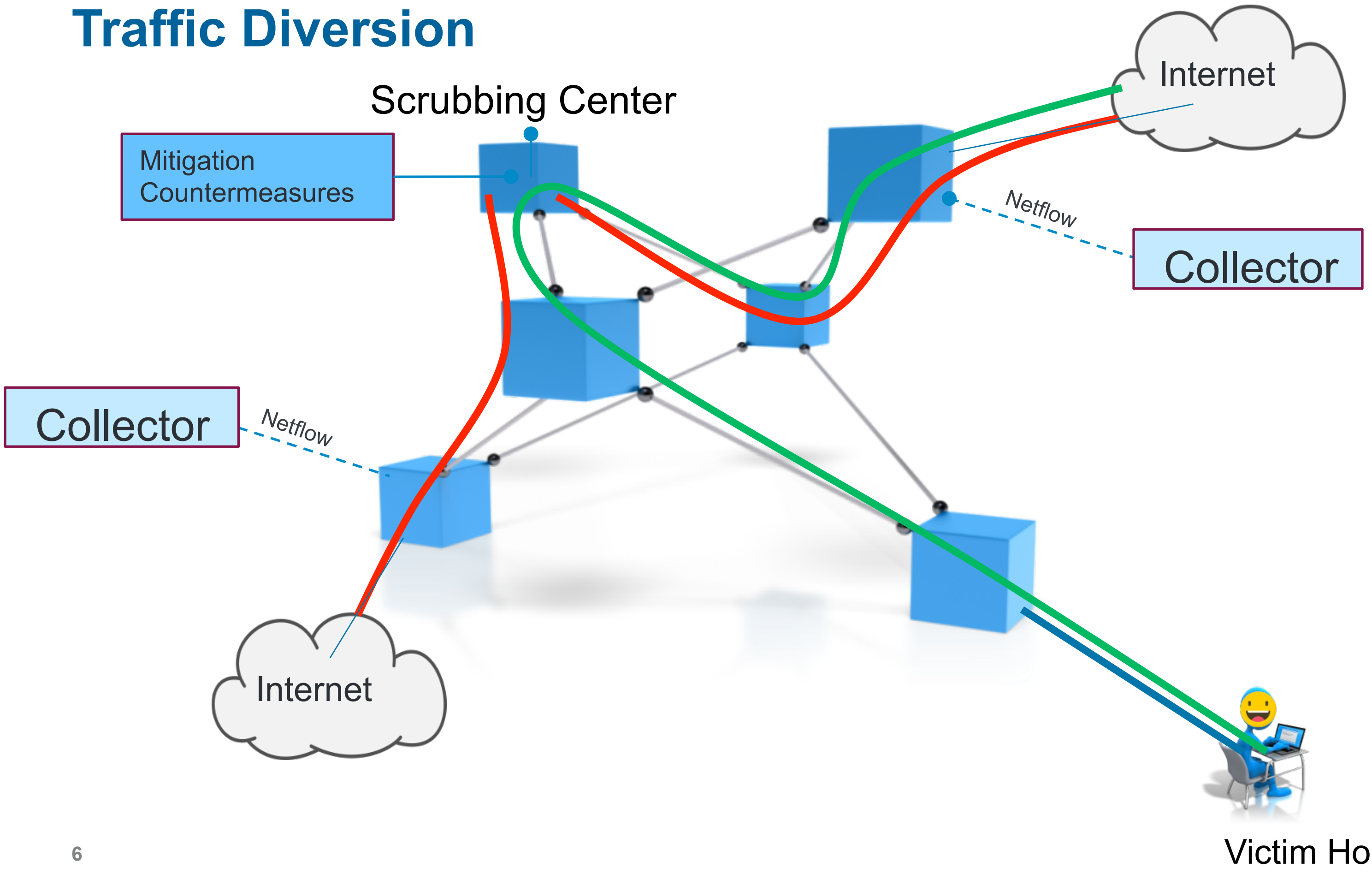
TRAFFIC DIVERSION METHOD (MOST COMMON)

- **Netflow collection and analysis**
  - Detection
- **BGP route injection**
  - Traffic Diversion
- **Scrubbing Appliance**
  - Traffic Mitigation
- **Clean traffic proceeds to the intended destination**
  - Traffic Reinjection

Traffic Diversion



Traffic Diversion



Proactive Mitigation

Blocking Ingress	Rate-Limiting Ingress
Source/Destination UDP Port 19 – Chargen	UDP Fragments
Source/Destination UDP Port 17 – QOTD	Source UDP Port 111 – SUNRPC
Source/Destination UDP Port 1900 – SSDP	Source UDP Port 161 and 162 – SNMP
Source/Destination UDP Port 520 – RIPv1	Source UDP Port 389 – LDAP
Source/Destination UDP or TCP Port 0	
Source UDP Port 123 Packet Length 468 –NTP	
Source UDP port 11211– Memcached	
Source UDP Port 53 – DNS	

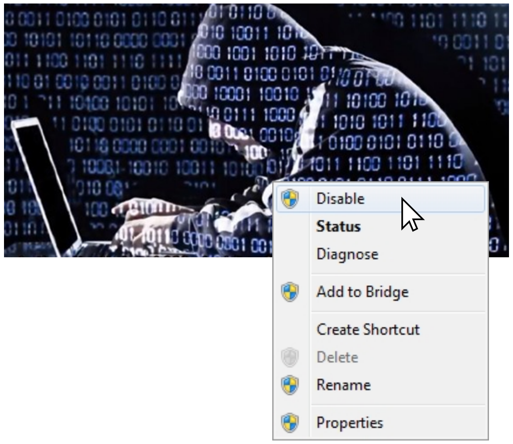
Proactive Mitigation Continued

BCP 38 and 84 - Network Ingress Filtering

- Designed to limit the impact of DDoS by identifying traffic with spoofed addresses

Always on Mitigations

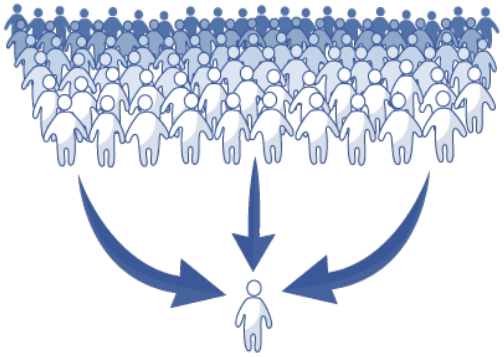
- Constantly divert traffic to a scrubbing appliance for mitigation
  - New attack vectors require human intervention



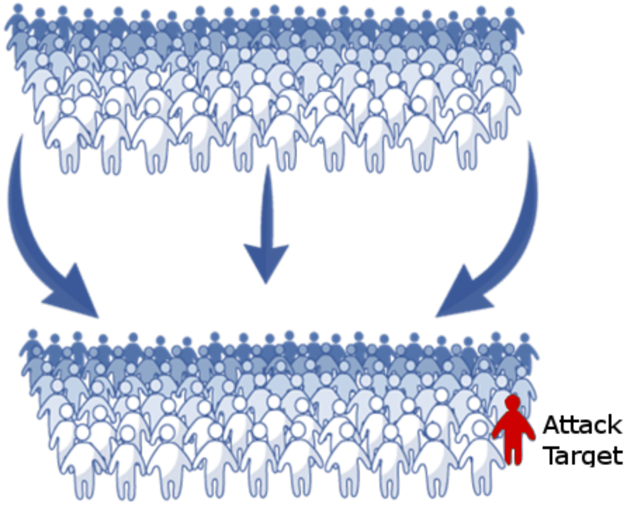
Challenges

“New” Attack Vector – Carpet Bomb

- Not really new
- Recent uptick suggests it’s becoming more popular
- Uses normal UDP Reflection/Amplification vectors
- Many-to-Many instead of Many-to-One
- Victim is among the crowd



Typical DDoS



Carpet bomb

Challenges Continued

More on Carpet Bomb Attack

- ➢ Attack targets large subnets (greater than /24)
- ➢ Very difficult to detect with netflow
- ➢ Traffic to individual hosts in the attack is too small to trigger a DDoS alert
- ➢ Saturates links at the customer edge
- ➢ Unable to utilize usual diversion techniques for thousands of hosts

Can we advertise that many host routes? Are there more preferential routes?
Do we have the scrubbing capacity to off-ramp that much traffic?

How can we block traffic closer to the source?

Enhancing DDoS Protection with Flowspec

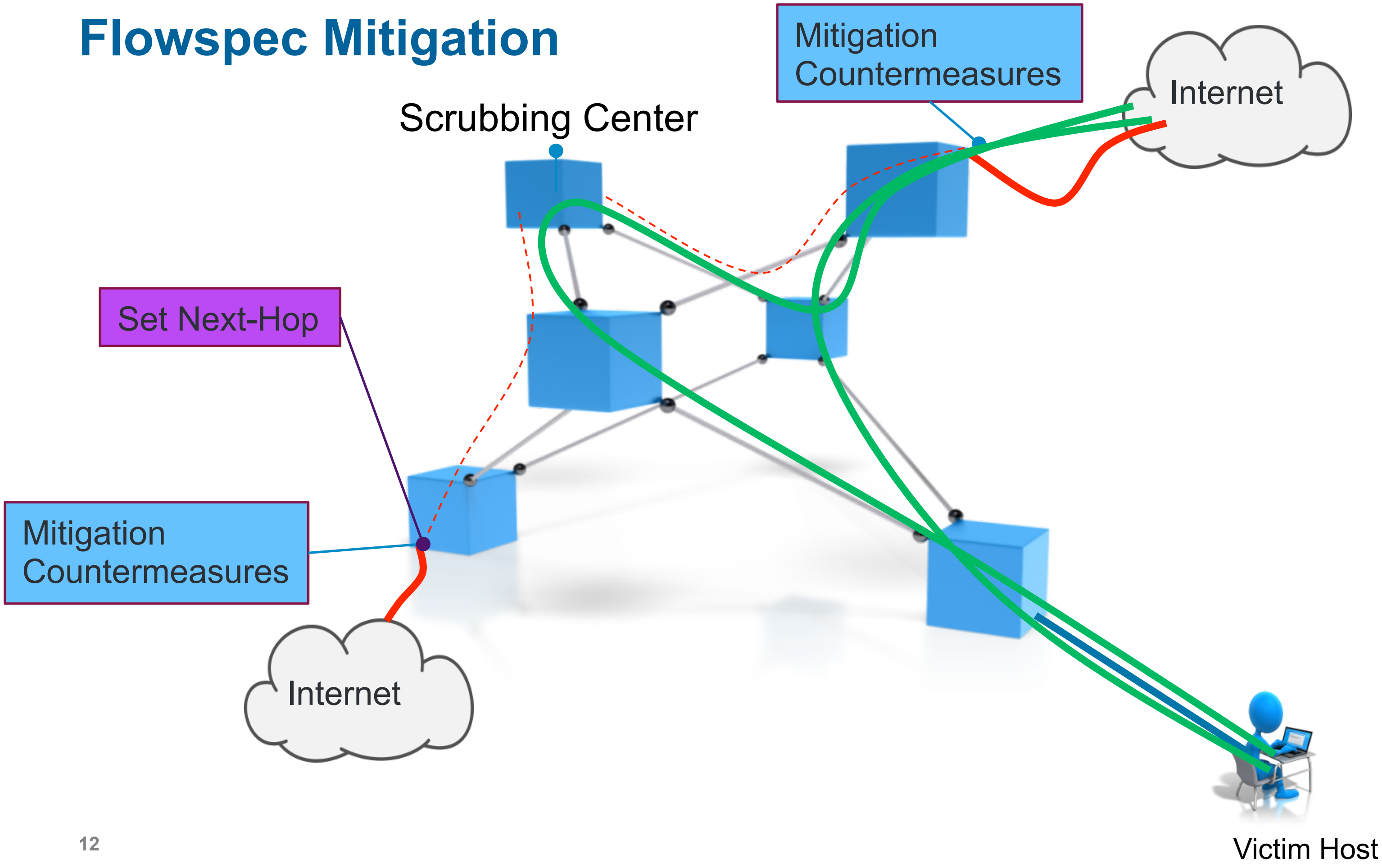
Pros

- Part of the BGP protocol
- Multi-Vendor support
- Quickly install mitigation rules
- Flexibility to specify traffic and action to pass, drop, rate-limit or set-next-hop
  - Port, Protocol, packet length, ICMP type/code, TCP flags, DSCP, Fragment encoding, IP source/destination

Cons

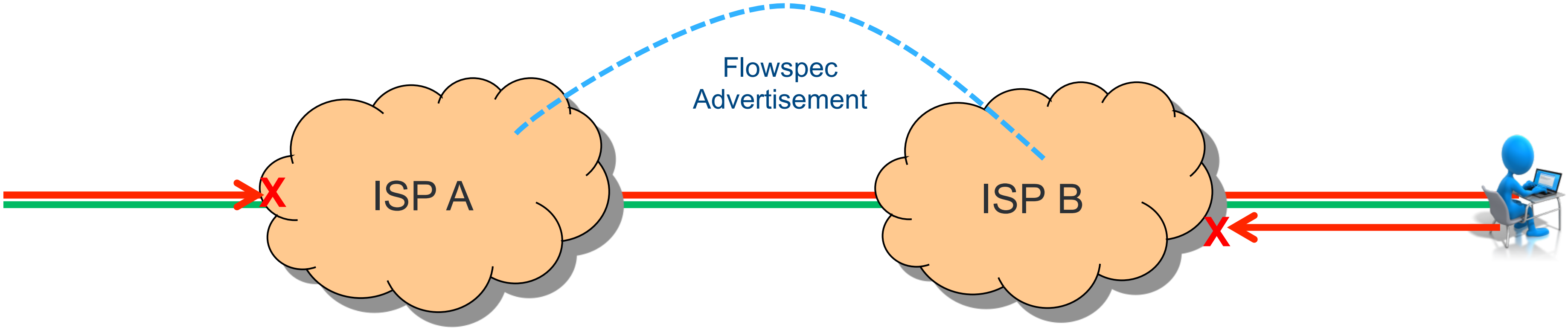
- Potential risk to router stability
- Gathering metrics is cumbersome
- Requires strong process/policy controls

Flowspec Mitigation



DDoS Peering with Flowspec

- Collaborative approach with other ISPs and Service providers
- Stop DDoS as close to the source as possible
- Allow Flowspec rules to be sent from peers
  - Huge Risks
  - Requires very tight controls
- Prevent customers from participating in DDoS attacks outbound



Automatic Flowspec Mitigation

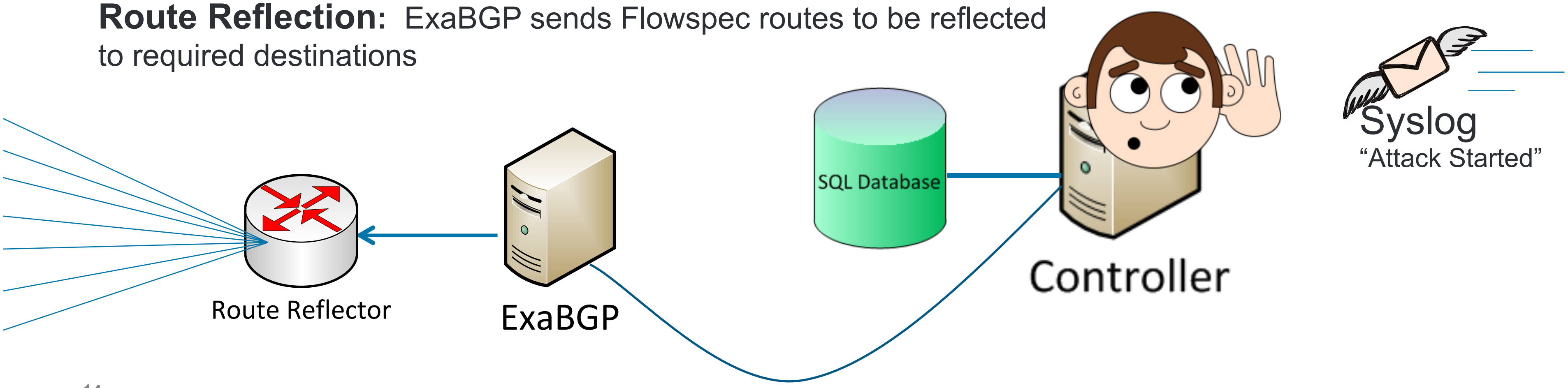
Controller – (Python)

Attack Detection: Listen for a syslog message from DDoS detection platform

Validation and Housekeeping: Look for keywords in the syslog message and store information in a SQL database (victim IP, active attack)

Mitigation Initiation: Send Flowspec rules to ExaBGP API

Route Reflection: ExaBGP sends Flowspec routes to be reflected to required destinations



Flowspec API call

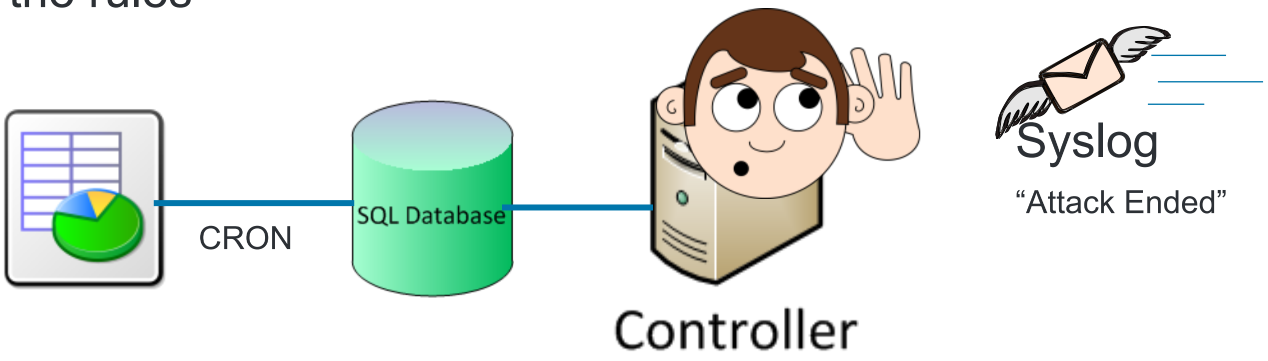
The Flowspec Rules

The script will generate the following rules for each IP under attack

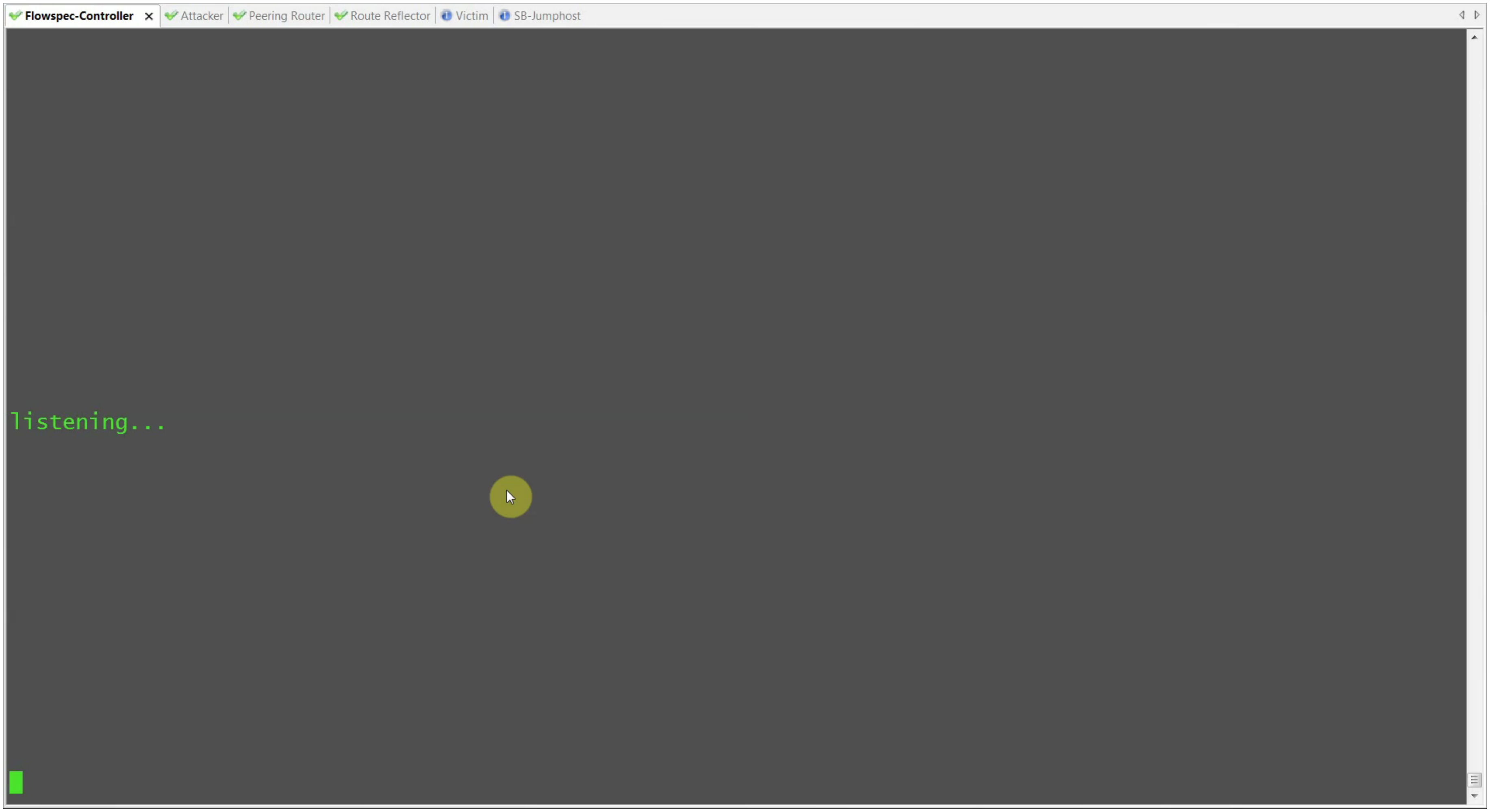
- ❑ Rate-limit UDP source-port 53 to 30Kbps
- ❑ Rate-limit ICMP to 30Kbps
- ❑ Drop UDP source-ports 69, 111, 137, 138, 161, 162, 389, 520, 1434, 1701, 5353, and 11211
- ❑ Drop UDP source-port 53 and destination-port 4444
- ❑ Drop UDP fragments
- ❑ Rate-limit TCP syn to 30Kbps
- ❑ Rate-limit all other traffic to 100Mbps

Clean-Up

- ✓ Once the attack has ended, we must withdraw the rules
- ✓ Controller listens for a syslog message indicating the attack traffic has stopped
- ✓ Query the database for the attack info and set ‘Inactive Attack’
- ✓ Send message to ExaBGP API to withdraw flowspec rules
- ✓ Cron job checks the database every hour for any active entry older than 6 hours and withdraws the rules



Auto Flowspec Script Demo



```
listening...
```

The End!

Questions?