CITYLINK™
TELECOMMUNICATIONS

# Using BGP and uRPF to Keep the Internet Secure

LACNIC / LACNOG 32, Panama City, Panama 2019

John Brown, CISSP

# About Me

- Based in Albuquerque, NM US.
- (ISC)2 CISSP and CISSP Certified (ISC)2 Instructor.
- Pushing packets for 30+ years.
- CEO/CTO of CityLink (regional telecom / hosting company).
- Fiber to the Home, Fiber to the Business.
- Past Technical Lead for ICANN’s  L-Root DNS Server.
- Certified technology instructor for several companies.
- Can spell BGP, TCP/IP, uDRP, etc :)
- Fly and build airplanes.

# Overview of topics

- How the Internet Moves Traffic Around
- Types of Traffic we want to stop
- Blocking Bad Traffic, Doing it at Scale
- Leveraging BGP, uRPF, RTBH methods to drop packets in hardware
- Example Configurations

# How the Internet Moves Traffic Around

# A Look Inside Routers

- Routers forward based on Destination IP Address
- Routers communicate with each other via a Route Advertising Protocol
- Internal protocols are  OSPF, ISIS, RIP (dead)
- External protocol used today is BGPv4, between autonomous systems.
- Two data sets are used by a router
  - RIB = Routing Information Base
  - FIB = Forwarding Information Base
- Router forwards based on what is in the FIB.  FIB is built from the RIB.
- If you can control the RIB/FIB you control how a router processes packets.

# Types of IP Traffic we want to Stop

# Source Spoofed IP Addresses

- What is Source Address Spoofing ?
  - It is the falsification of the packets Source IP Address.
- When do we know the Source Address is Fake ?
  - At the first point the packet is injected into the network from the client device.
- How do we prevent Source Spoofing ?
  - IETF / BCP 38, written 20 years ago!!
- In today’s global internet we need better network HYGIENE!
- MANRS is something we all should read and subscribe to!
- DNS / NTP are two great examples of Attacks that leverage Source Spoofed IP’s

# BOTNET / C2 / and more

- We can leverage IP Reputation data to block other types of bad traffic
- BOTNET's
- Command and Control (C2) servers
- Bad DNS Servers
- Other hosts you don't want to talk to.
- Two examples of where you can get IP reputation data from


# Blocking bad traffic, Doing it at scale

# Preventing Spoofed Packets on your network

- You can write filter rules (ACL's) for your routers.  This can impact CPU.

- You have to apply the ACL's to each interface on your entire network.

- Not very easy to maintain, prone to errors.

There must be a better way……..

# Dropping DDOS traffic to a victim host

- You can write filter rules (ACL's) for your routers.  This can impact CPU.
- You have to apply the ACL's to each interface on your entire network.
- Not very easy to maintain, prone to errors.

There must be a better way……..

# Preventing BOTNET C2 and other things

- You can write filter rules (ACL's) for your routers.  This can impact CPU.

- You have to apply the ACL's to each interface on your entire network.

- Not very easy to maintain, prone to errors.

There must be a better way……..

# Better Ways

Destination based filtering

Source based filtering

# Destination Based Filtering

- We know that routers make decisions based on the FIB
- By placing a bad IP into the FIB we can control how a packet is forwarded
- So we can use BGP to “inject” a bad IP into all of our routers.
- We place a “This is a BAD IP” Tag (community string) on the injected route.
- All of our routers insert this Bad IP into the FIB with a NXT-HOP of NULL
- Now packets Going TO this bad IP are dropped.
- In many cases this is done in hardware and has very little impact on CPU.
- If you make arrangements with your transit providers, you can use BGP to tell them to drop traffic towards you.  This is what a RTBH is.
- RTBH == Remote Triggered Black Hole

# Preventing Source Spoofing

- IETF’s BCP 38 addresses how to prevent Source Spoofed Packets.
- You have to catch the spoofed packet as it enters your network from a customer.
- uRPF is used to help prevent source spoofed packets.

# What is uRPF

uRPF = Unicast Reverse Path Forwarding

Defined in IETF RFC 3704

uRPF is designed to limit the impact of distributed denial of service attacks, by denying traffic with spoofed addresses access to the network.

# How does uRPF work?

- Routers typically make decisions based on Dest IP
- With uRPF, router now also looks at Source IP.
- Two Modes  (Strict and Loose)
- Router looks at Source IP and then the routing table.
- If source is reachable via the input interface, then good, else drop (Strict)
- If source reachable via any route in routing table, then good, else drop. (Loose), except null.
- If nxt_hop is null, then DROP packet.

# Use uRPF (Loose) Feature

- What you can do is use a part of uRPF/Loose
- Inject route into your FIB (Forwarding Info Base)
- Have the next hop of that route be BLACKHOLE
- uRPF/Loose will see Nxt_Hop is Blackhole and DROP.
- So you inject the Src_IP's of the bad traffic with Nxt_Hop as Blackhole, magically, traffic FROM (Source) goes away at your edge.
- You can use tools to create real-time injects.
- exa-BGP is nice open source tool to do the BGP injection

# Filtering Spoofed Packets from your customers

- TEST THIS IN A LAB FIRST

- Enable uRPF Strict on your single homed customer interfaces
  - Will prevent spoofed packets from entering your network from your customer
  - Will prevent your customer from participating in a DDOS
  - Will keep the Net cleaner (better Hygiene)
  - Will save you money (less wasted bandwidth, really important to WISP’s)

- This can break your network, so please TEST THIS IN A LAB FIRST

# How to inject bad prefixes into BGP

- We need a BGP daemon, a program that speaks the BGP protocol.
- We need the ability to make changes in real-time.
- It needs to be easy to configure and operate.

## EXA-BGP

- Can run in a simple Linux VM
- Supports real-time configuration changes
- Has hooks that allows other programs to “feed it” data.
- Support text or JSON feeds

# CAUTION CAUTION CAUTION CAUTION

- You *MUST* NOT redistribute these “bad IP’s” to your peers or transit providers.

- DANGER DANGER DANGER TEST THIS IN A LAB FIRST!!!

- Make sure your BGP-OUT filters DROP all prefixes with your “Bad_IP” community tag!!!!!!

# EXAMPLE CONFIGURATIONS

# Juniper Router Configuration / Edge uRPF

```
Interface ge-1/0/0
unit 0 {
   family inet {
        rpf-check {
            mode loose;
        }
        filter{
            input-list ce-in;
            output-list cust-drop;
        }
        sampling {
            input;
        }
        address XXX.XXX.XXX.XXX/30;
   }
}
```

# Juniper Router Configuration / exaBGP Neighbor

```
group eBGP-PEER-AS65555-exaBGP-RTBH {
    type internal;
    local-preference 800;
    local-address 192.168.111.1;
    family inet {
        unicast;
        flow;
    }
    cluster 192.168.111.1;
    neighbor 192.168.111.42 {
        accept-remote-nexthop;
        peer-as 65555;
    }
}
```

# Exa-BGP Route Announcement

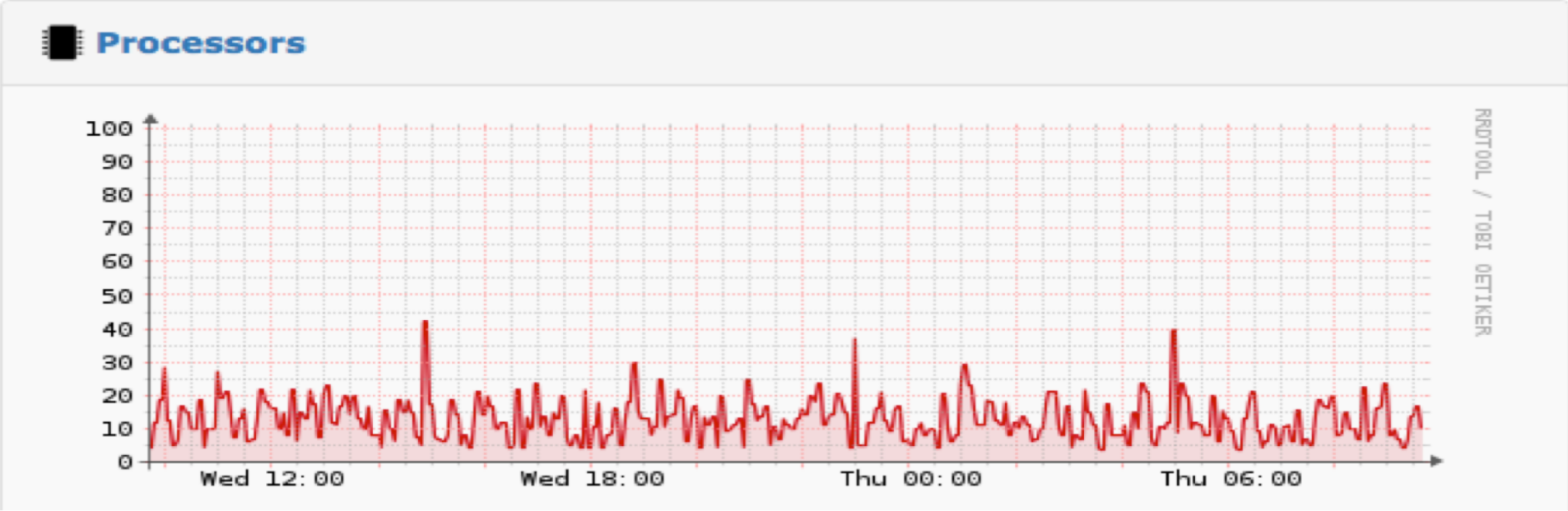
```
route 45.35.208.226/32 next-hop 192.0.2.1
  community [65001:666 65001:400]
  local-preference 5000;
```

This can be sent via JSON or text to exa-bgp

# Juniper Route Entry

```
45.35.208.226/32   *[BGP/170] 37w0d 18:16:07, localpref 5000, from 192.168.111.42
                    AS path: I, validation-state: unverified    to Discard
```

# CPU Load Graph, 40,000 bad IP’s



# Closing Summary

- Using tools like exa-bgp, uRPF and the BGP protocol we can protect our net
- Understanding how uRPF works can better protect your network.
- We have shown how to drop traffic based on BOTH Source and Dest IP Addr.
- Each of us has a responsibility to doing our part to keep the Internet clean
- Please make sure you apply BCP 38 to YOUR network.
- Read up on MANRS and Join if you feel it is appropriate.

# Some resources / tools

exaBGP https://github.com/exa-networks/exabgp

Team CYMRU

UTRS https://www.team-cymru.com/utrs.html

BOGON https://www.team-cymru.com/bogon-reference.html

Reputation Feed https://www.team-cymru.com/controller-feed.html

QUESTIONS / DISCUSSIONS ??