BGP operational security best practices

Jérôme Durand – Consulting Systems Engineer

BRKRST-2045

Agenda

- Why ?
- Protect your router and sessions
- Basic policies
- IXP specifics
- IRR lockdown
- RPKI and route origin validation
- BGPsec

For IPv4 and IPv6

Usual best practices

Focus of this session

There is an RFC now

Internet Engineering Task Force (IETF)
Request for Comments: 7454
BCP: 194
Category: Best Current Practice
ISSN: 2070-1721

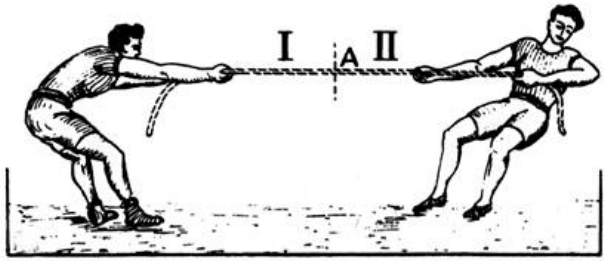
J. Durand
Cisco Systems, Inc.
I. Pepelnjak
NIL
G. Doering
SpaceNet
February 2015

BGP Operations and Security

Abstract

The Border Gateway Protocol (BGP) is the protocol almost exclusively used in the Internet to exchange routing information between network domains. Due to this central nature, it is important to understand the security measures that can and should be deployed to prevent accidental or intentional routing disturbances.

IPv4 address exhaustion



Datacenter

IPv6

Cloud and IXP

Protect your routers and TCP sessions

- TTL Security (GTSM)
  - TTL 1 by default for EBGP – Send with TTL 255 and deny anything with TTL < 254
- MD5 peers authentication
- Infrastructure ACL
  - Control traffic to your own infrastructure
- COPP / LPTS
  - Policy traffic reaching your control plane

Basic policies

- Martians
- Maximum prefixes limit
- Prefix length
- First AS in AS-Path
- Route Flap Dampening

IPv6 specifics

- What is same
  - IPv6 is IP – same kind of procedures
- What is different
  - Different address types
  - Registries

Closer look on IXPs

- The IXP LAN prefix
- pMTUd and uRPF
- Next-hop enforcement
- Deal with BGP route servers

IRR lockdown

- Tie rules to IRR objects
  - AS-SET ➔ AUT-NUM ➔ ROUTE(6) ➔ INETNUM(6)
- IRR accuracy
  - IRRexplorer
- Demo

RPKI / ROA and BGPsec

- RPKI / ROA principles
  - Validators
  - RTR protocol
  - Policy definitions
- Demo
- Future work: BGPsec

Thank You

Cisco live!