CCIE Security Version 5
Advanced Technologies Class

Remotely Triggered Black Hole

What is RTBH?

What are the deployment options?

RTBH Overview

- RTBH
  - It's a packet filtering technique that allows dropping undesirable traffic at the edge of your network
  - It's used to stop DoS and DDoS attacks
- RTBH
  - Relies on remote iBGP updates in order to black hole traffic
  - Works for both IPv4 and IPv6 packets

RTBH Overview

- RTBH can black hole the traffic based on
  - Destination IP address of the packet
  - Source IP address of the packet

Destination Based RTBH Overview

How does it work?

- All edge iBGP routers have a Null0 route for a prefix (RFC 6666 defines the discard prefix for IPv6)
- When a destination is under attack, a BGP speaker called the trigger router, will trigger an iBGP update
- This update contains a route for the attacked destination with a next-hop of the prefix which is Null0 routed

Destination Based RTBH Overview

- What is the outcome?
  - All traffic towards that destination is dropped inbound at the edge of your network

Destination Based RTBH

- Implementation steps
  - Have iBGP configured
  - Configure the Null0 route on your edge iBGP routers
  - When under attack, trigger the iBGP update for the destination of the attack
- Optionally, but recommended
  - Disable IP unreachable to avoid high CPU

Source Based RTBH Overview

How does it work?

- All edge iBGP routers have a Null0 route for a prefix (RFC 6666 defines the discard prefix for IPv6)
- All edge iBGP routers have uRPF in loose mode configured
- When a destination is under attack, a BGP speaker called the trigger router, will trigger an iBGP update
- This update contains a route for the source of the attack with a next-hop of the prefix which is Null0 routed

Source Based RTBH Overview

- What is the outcome?
  - All traffic from the source of the attack is dropped inbound at the edge of your network

Source Based RTBH

- Implementation steps
  - Have iBGP configured
  - Configure the Null0 route on your edge iBGP routers
  - Configure uRPF in loose mode on your edge iBGP routers
  - When under attack, trigger the iBGP update for source of the attack
- Optionally, but recommended
  - Disable IP unreachable to avoid high CPU

RTBH Comparison

- Destination based RTBH
  - Drops all incoming traffic for the destination of the attack (legit and malicious)
  - Good in DDoS when there are too many sources
- Source based RTBH
  - Drops all incoming traffic from the sources of the attack, legit traffic still works
  - Good in DoS or DDoS with not too many sources