CCIE Security Version 5 Advanced Technologies Class

IP Address Spoofing

What is IP address spoofing?

How can IP address spoofing be mitigated?

IP Address Spoofing Overview

▷What is IP address spoofing?

- When a host/user spoofs the layer3 identity (IPv4/IPv6) of another host

▷How is this used?

- In general for DDoS and DoS attacks
- Legit use-case would be with HTTP/HTTPS proxy deployments

▷How can it be mitigated?

- RFC 1918, RFC 2828, RFC 3330
- uRPF (Unicast RPF)

RFC 1918 Overview

- RFC 1918 defines the private IPv4 address space
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- How can it defend against address spoofing?
  - Internet traffic should have a public IPv4 source address
  - Configure inbound IPv4 filter from the Internet and drop traffic sourced with RFC1918 addresses
  - Optionally configure ACL logging to be notified of attacks

RFC 1918 Overview

▷Considerations

- Filtering is always done ingress by the customer/ enterprise
- Ingress ACL may have exceptions (BGP peering with the ISP on private IPv4 addresses)

RFC 2827 Overview

- RFC 2827 defines an IPv4 filtering method
  - For Internet traffic, the source IPv4 address needs to be within the customer's allocated public address space
- How can it defend against address spoofing?
  - IPv4 traffic sourced from illegal addresses is dropped
- Considerations
  - Ideally, filtering is done inbound by the ISP
  - Optionally, it can be done outbound by the customer/ enterprise

RFC 2827 Overview

- RFC 2827 is updated by RFC 3704 which states
  - IPv4 traffic with martian source addresses must be dropped
- Martian address
  - IP address space reserved for special purposes
- Martian address examples
  - RFC 1918
  - IPv4 Loopback range 127.0.0.0/8
  - IPv4 multicast range 224.0.0.0/4

RFC 3330 Overview

- ▷RFC 3330 (obsoleted by RFC 5735) defines
  - IPv4 address space reserved for special purposes
- ▷RFC 5156 defines
  - IPv6 address space reserved for special purposes
- ▷RFC 5735 and RFC 5156
  - Obsoleted by RFC 6890
- ▷RFC 6890 defines
  - IPv4/IPv6 address space reserved for special purposes

Knowledge is Power!