CCIE Security Version 5 Advanced Technologies Class

Fragmentation Attack Protection via ACL

How can ACL’s stop fragmentation attacks?

How are fragments processed against IP ACL’s?

IPv4 vs. IPv6 Header

- Quick comparison:
  - http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Fragments Filtering via ACL

- How can ACL drop fragments?
  - By using the '**fragment**' keyword attached to your ACE, it matches on non-initial fragments
- What are the challenges with filtering fragments via ACL?
  - For both IPv4 and IPv6, non-initial fragments do not contain layer 4 information
- ACL and IP fragments matching
  - http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/8014-acl-wp.html

Fragments Filtering via ACL

- ▷How can ACL drop fragments?
  - By using the '**fragment**' keyword attached to your ACE, it matches on non-initial fragments
- ▷What are the challenges with filtering fragments via ACL?
  - For both IPv4 and IPv6, non-initial fragments do not contain layer 4 information

Fragments Filtering via ACL

- ACL and IP fragments matching
  - http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/8014-acl-wp.html
- What is the issue with fixing fragmentation attacks via ACL, CAR, policing, packet discard?
  - All fragments are dropped, both good and bad

Knowledge is Power!