Intrusion Detection System

IDS Overview

ACI Virtual Edge (AVE) provides IPv4 Intrusion Detection System (IDS) packet checks to increase security in the network by dropping packets that match specific criteria that are typically not required in most production networks. IDS packet checks are enabled by default and should be left enabled unless there is a specific reason to disable them.

Guidelines and Limitations for IDS

This section describes the guidelines and limitations for IDS:

- IDS can be disabled by logging into to AVE and run the `vemcmd set ids disable` command.

Note This is not persistent upon AVE reboot.

There is no knob in the APIC GUI to turn this feature on or off.

IDS Check

The following packet validations are done by IDS:

- consistency checks between frame length, IHL, Total length (no strict)
  - IHL >= 5
  - payload length + 8*frag_offset <= 64K
  - If DF==1 then must have frag_offset == 0
  - Invalid packet padding
  - disallow SA == 255.255.255.255
  - disallow SA == 127.x.x.x
  - disallow DA == 127.x.x.x

```
- disallow IPSA = IPDA
- disallow DA = 0.0.0.0
- disallow SA of class D
- disallow SA of class E
- disallow DA of class E
```