Next Generation Firewall Performance Testing

Timothy Winters, twinters@iol.unh.edu

IETF 106, Singapore, November 2019
Network Security Device Performance

• Creating Performance Testing for Next Generation Firewalls to better align with the current Firewalls.
  – Last IETF draft for benchmarking firewalls was 15 years ago.

• Must of the work has been happening in the NetSecOpen Next-Generation Firewall Testing Methodology.
  – Includes members from 2 labs, 3 tool vendors, and 8 firewall members.
Beta Testing

• On-going activity
  – Several Firewalls are undergoing testing at both UNH-IOL and EANTC.
  – Comparing measurements from multiple tools.
  – Comparing measurements of the different firewalls.
Updated Firewall Configuration

• Updated the configuration of ACLs on the firewall to MUST from SHOULD.
  – Users will most likely have ACLS configured on the Firewall and will want to see performance numbers based on that.

• Updated Traffic logging from all traffic to all flows.
  – Users don’t need to see every packets but really the flow, and logging all the packets impacts performance.
Measurement

• Removed Application Transaction Latency
  – Not clear if this was the best KPI so we removed it.
  – Anywhere is was measured we suggested other criteria.

• Removed Extra KPIs that weren’t necessary.
  – Example, Updated 7.2 (TCP/HTTP) to only look for Average TCP connections.