Packet Optimization & Visibility with Wireshark and PCAPs

Gordon Beith
Director of Product Management
VSS Monitoring
Market Trends - Innovation

• In a hyper connected world, one must master the trends of cloud, virtualization, SDN, media, mobile, business intelligence while overcoming security threats.

• This makes Network, Application, and Security monitoring and analysis tools critical to have…
Monitoring & Analysis Challenges

- Access to all key points in the network
  - Is a tool (e.g. Wireshark) instance at every point realistic?
    - Costly to install and maintain
    - Difficult to manage across different locations
    - Won’t get full picture/session, e.g. asymmetrical routing
    - High speeds, e.g. 40G, & 100G, probably not accessible

- Visibility to all required packets from the network
  - Can a single tool instance handle all traffic?
    - Total bandwidth is too much for NICs and processors
    - Each instance of a tool probably doesn’t need to see all traffic
  - Can a specific tool understand all protocols?
    - Tunneling and virtualization protocols often not supported nor interesting
    - Encrypted traffic content typically not accessible to tools
Monitoring & Analysis Challenges (2)

- **Scalability of Tools**
  - How can a tool scale to meet increasing traffic and number of networks?
    - Next to impossible without faster processors, bigger disks, and more/higher-end NICs

- **Impacts of Bursty Traffic**
  - How can effects of microbursts be mitigated?
    - Needs to be done in the aggregation hardware to avoid packet loss

- **Governance and Legal Compliance**
  - In what ways can tools comply with HIPPA, LI, PCI, SOX, etc.?
    - Very difficult without programmable hardware pre-processing in tool

➤ Employ Network Packet Brokers!
What are Network Packet Brokers?

- A newer type of network appliance
- Sits between network and intelligence tools
- Captures network traffic at line rate
- Grooms packets ready for network intelligence tools
- Forwards packets to network intelligence tools
Addressing the Challenges with NPBs

- Network & Traffic Access
  - Deploy network TAP appliances wherever possible
    - Remove Mirror/SPAN port contention
    - Ensure reliability of data access
    - Use Mirror/SPAN ports on switches/routers if no other choice
  - Employ virtual Mirror/SPAN/TAP points within virtual environments
    - Direct traffic out from virtual environment
Addressing the Challenges with NPBs (2)

- **Traffic Delivery Optimization**
  - Deploy Network Packet Brokers (NPBs) as a complete system
  - Either as a second tier or with TAPs integrated
  - Selective aggregation from access towards monitoring tools
  - Filter traffic based on layers 2 to 7, with/without tunneling
  - Balance traffic across multiple tools maintaining session integrity
  - High availability & redundancy

- **Include Microburst Detection & Mitigation**
  - Visibility to granular traffic profile for network capacity planning
  - Ensure delivery of all monitored packets despite microbursts
Addressing the Challenges with NPBs

- Packet Optimization
  - Port and Time Stamping
    - Visibility to packet’s source link and time of occurrence
    - Accuracy is important
  - Protocol De-encapsulation/Stripping
    - Remove unwanted/unsupported protocol headers from monitored packets, e.g. GTP tunnels, MPLS labels, VLAN tags, VN-tags
- Conditional Slicing
  - Remove unwanted/undesirable data from specific packets
  - Support regulatory and legal compliance
Addressing the Challenges with NPBs

• Packet Optimization
  – De-duplication
    • Minimize bandwidth required for delivery
    • Improve on tools’ efficiency and accuracy
  – Fragment Reassembly
    • Facilitate flow/session-based balancing and filtering of traffic
    • Improve tool efficiency and accuracy
  – SSL Decryption
    • Visibility into encrypted traffic
Addressing the Challenges with NPBs

- **PCAP Creation Optimization**
  - Encapsulate packets in PCAP file format
    - Include metadata (e.g. accurate timestamps and source port) in PCAPng format
  - Forward to network-attached storage device for analyzer tools to access, or... stream to tool
Interpreting Results in Wireshark

- **Port Stamping**
  - End-of-packet
    - Trailer after and of IP packet
    - Minimizes added bytes
  - Start-of-packet
    - VLAN tag alternative

- **Time Stamping**
  - End-of-packet
    - Trailer after and of IP packet
    - Minimizes added bytes
Interpreting Results in Wireshark (2)

- Time and Port Stamps in Trailer example

- Port Stamp in VLAN Tag example
Interpreting Results in Wireshark

- **Protocol Stripping/De-encapsulation**
  - **GTP Tunneling**
    - Remove all 3 headers
  - **MPLS Tunneling**
    - Remove all labels and/or encapsulation
  - **VLAN & VN Tagging**
    - Selectively remove 1, 2, or all tags
    - Remove all or only specific TPID tags
Interpreting Results in Wireshark (4)

- GTP Tunneling example
  - With GTP Encapsulation
  - With GTP Encapsulation Removed
Interpreting Results in Wireshark (5)

- MPLS Tunneling example
  - With MPLS Labels
    - Frame 3: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
    - Source: Cisco_05:28:38 (00:30:96:05:28:38)
    - Type: MPLS label switched packet (0x88a7)
    - MultiProtocol Label Switching Header, Label: 245, Exp: 0, S: 0, TTL: 64
      - 0000 0000 0000 1111 0101 ....... = MPLS Label: 245
      - .... .... .... .... 000. .... = MPLS Experimental Bits: 0
      - .... .... .... .... 0 .... = MPLS Bottom of Label Stack: 0
      - .... .... .... .... 0100 0000 = MPLS TTL: 64
    - MultiProtocol Label Switching Header, Label: 227, Exp: 0, S: 1, TTL: 64
    - Internet Protocol Version 4, Src: 10.31.85.1 (10.31.85.1), Dst: 10.34.85.1 (10.34.85.1)
    - Data (56 bytes)
  - With MPLS Labels Removed
    - Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
    - Source: Cisco_05:28:38 (00:30:96:05:28:38)
    - Type: IP (0x0800)
    - Internet Protocol Version 4, Src: 10.31.85.1 (10.31.85.1), Dst: 10.34.85.1 (10.34.85.1)
    - Data (56 bytes)
Interpreting Results in Wireshark

- VLAN & VN Tagging example
  - With VLAN Tags
  [Image of Wireshark frame with VLAN tags]
  - With VLAN Tags Removed
  [Image of Wireshark frame with VLAN tags removed]
Interpreting Results in Wireshark

- Conditional Packet Slicing
  - Single out specific packets or traffic types
  - Slice packet contents from specified point in packets

<add Wireshark decoded vSliced packet>
Interpreting Results in Wireshark

- **Packet De-duplication**
  - Forwards on unique packets
  - Drops all subsequent duplicates with specified time window
  - Expect to see missing sequences

- **IP Fragment Reassembly**
  - Reassembles “outer” fragments
    - Any IP packet
  - Reassembles “inner” fragments
    - Encapsulated fragmentation, e.g. IP within GTP, IPv4 within IPv6
  - Expect to see missing sequences
Interpreting Results in Wireshark

- **SSL Decryption**
  - Detect and decrypt all SSL flows/sessions
  - Forward all clear text/decrypted packets to monitoring & analysis tools
Interpreting Results in Wireshark

- SSL Encryption example

![Wireshark Screenshot]
VSS Portfolio

TAP Series
Standard passive & active Taps for SPAN, in-line regeneration, replication & aggregation

vBroker™ Series
High capacity flexible packet brokers that provide network-wide visibility, data access and optimization for network monitoring and security tools; both passive and active inline.

vInspector™ Series
Bidirectional, high throughput SSL decryption and re-encryption appliances

VSS Management Center (vMC™)
Network-level management console (MC) for managing VSS packet brokers and TAPs, providing network-wide topology views, configuration, policy mgmt, reporting, and administration/updates.
Summary

Monitoring for Performance and Security is absolutely necessary

- But there are challenges…
- Challenges are increasing as network speeds and data increase

Network Packet Brokers are critical to addressing the challenges

- Address most, if not all, challenges

► Wireshark can be used with VSS’ Network Packet Brokers as an excellent troubleshooting, monitoring, and analysis solution!