Rethinking Cyber Security

The Need for a Packet Delivery Platform

Allen A. Hébert

Corporate Blogger / Senior Systems Engineer

Gigamon

allen.hebert@gigamon.com

(512) 657-5449

Bad Actors are Very Smart

- Criminals are Smart
- They are usually one step ahead of us
- Our Defenses have to work 100% of the time
- The Attacker only has to be successful once

- We need to have multiple lines of defense, defending and protecting our computing environments

Knowledge is Power in Cyber Security

- The more information you have, the better you can do your job
- Security Operations involve a lot of technologies designed to protect your computing environment
  - Physical Security
  - Network Perimeter cybersecurity (Firewalls, Malware Protection, Intrustion Prevention Systems, etc)
  - Internal Network Security (Intrusion Detection System, Packet Flow Analysis)
  - Endpoint Security (Antivirus, Anti-malware, Host Firewall)
  - Website/Database security
  - Application Security
  - Encryption
  - Layer 8 Security
- Network Packets provide a view into the “heart beat” of your computing environment

The Good Old Days

- Fault management was the easiest to implement
  - HP Openview/Netview, Spectrum, Whats Up Gold
  - Primarily network topology and configuration backups
- Configuration management was second
  - Vendor Provided Management software
- Performance Management was a distant third
  - RMON was a good first try to gain visibility into traffic behavior and performance of the network
- Security Management was not even on the radar.
  - Firewall and Anti-Virus on the end points

The Good Old Days cont.

- All solutions had to be closely watched to ensure that the monitoring did not adversely affect the production traffic
- Mostly in-band management and many times reactive verses proactive approach
- Gathering useful information on trends was laborious and time consuming and required lots and lots of expertise to interpret the data

Methods of Managing the Network

- There are Two Primary Routes to Secure Your Network
  - Device Based Security
  - Traffic Analysis

Device-Based Security

- Data is collected from devices on the network via the Production Network
  - Routers/Switches, other networking equipment
  - Servers
  - End User Workstations
- Collected data includes security logs, fault, performance, troubleshooting and diagnostic information of the device being monitored

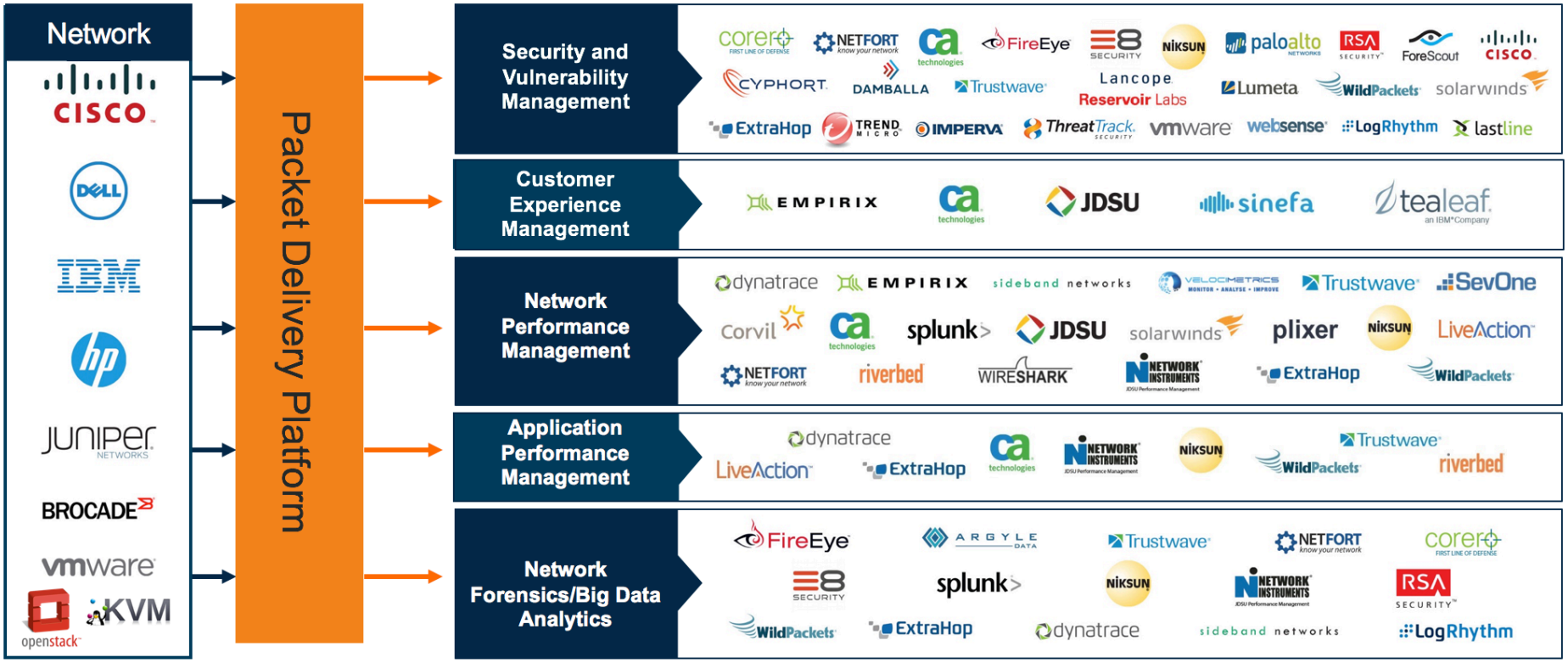
Device-Based Management Examples

- Network Manager of Manager Systems - HP OpenView, OpenNMS, CA Spectrum, SolarWinds and many others
- SEIM (Security information and event management) Tools - LogRhythm, Splunk, and many others
- All Manufacturer Management Software

Traffic-Based Management

- Data is collected using non-production links (TAPs and SPANs)
- The collected data to be analyzed is the traffic (packets) traversing the network
- Packets don’t lie
- Network Packets show everything
- Packets can be converted into MetaData

Example of Traffic Analysis Tools



Gigamon

Security Market Segments & Key Players

Data Loss Prevention
RSA
Symantec
Websense

Secure Email Gateways
Cisco
Intel (Mcafee)
Proofpoint
Sophos
Trend Micro

Web App Firewall
Imperva
F5
Citrix

Next-Generation Firewalls
Check Point
Cisco
Fortinet
Juniper
Palo Alto Networks

Forensics
ExtraHop
Niksun
RSA
Savvius

Secure Web Gateways
Blue Coat
Symantec
Websense

User Behavioral Analytics
Damballa
Lancope
LightCyber
Niara

Network Access Control (NAC)
Cisco
ForeScout
Juniper

SIEM
HP ArcSight
LogRhythm
RSA
Splunk

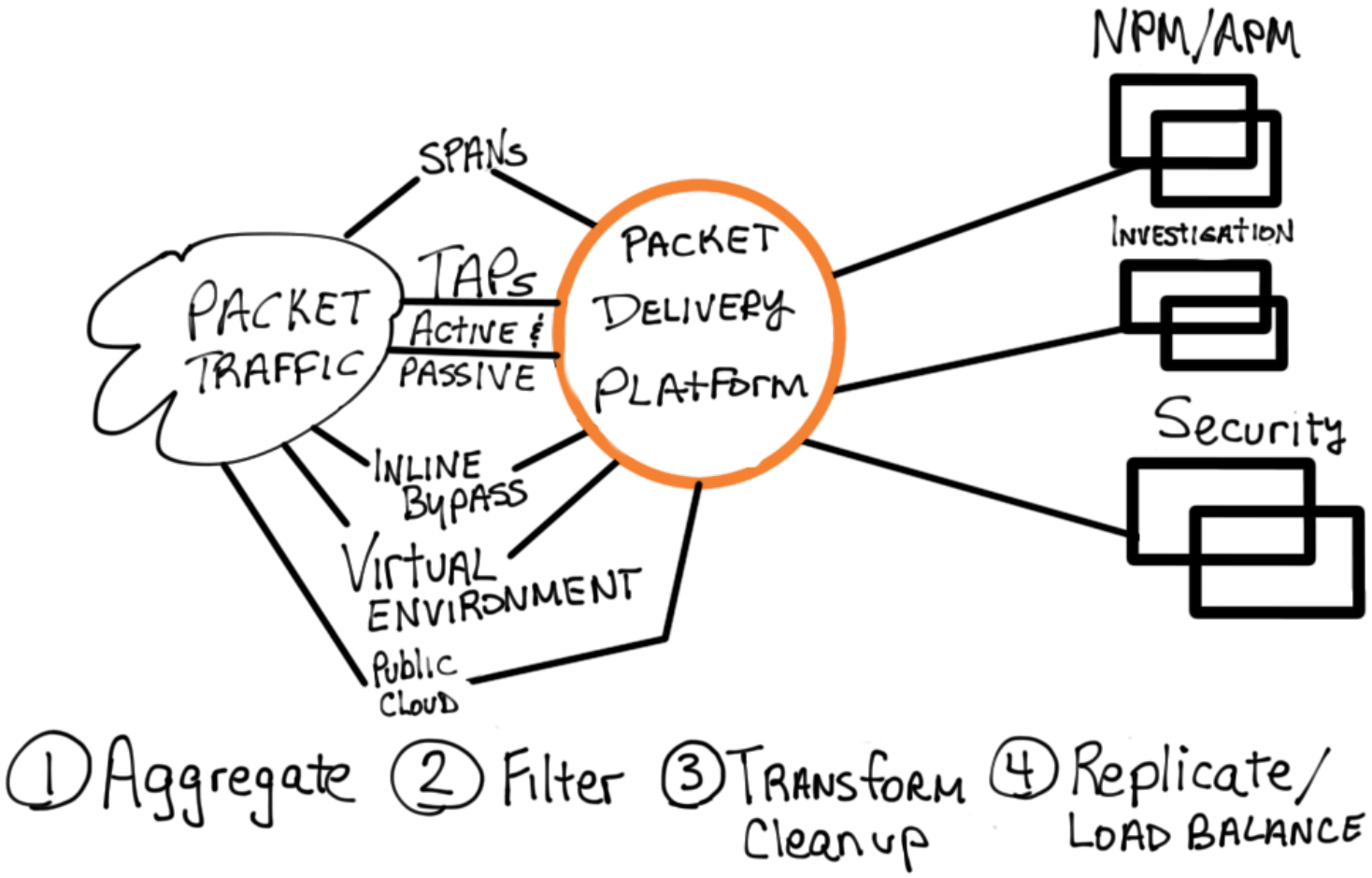
Standalone IDS / IPS
Blue Coat
Check Point
Cisco
Corero
HP
IBM
Tenable

Malware Protection / Sandboxing
Check Point
Cisco
Cyphort
FireEye
Lastline

Metadata for Security

- AKA NetFlow or IPFIX
- NetFlow metadata provides important information about network conversations and behavior.
- Each unique flow is reported to a metadata data collection server.
- The flow information, while lacking payload data, still provides enough data to the security professional to be a valuable analysis tool.
- The data is compact, can be stored for multiple months or years.
- Provides forensic capability, real-time analysis of traffic flows, connection information and shows abnormal network behavior.
- This data can be used both for intrusion detection and for incident handling purposes.

Packet Delivery Platforms



Gigamon

Your Tools Deserve a Solid Foundation

Choosing the right traffic source for each tool.

Knowing how reliable the traffic stream is which reaches your monitoring and security tools can be as important as the quality of the analysis being performed on that traffic.

Five traffic sources will be explored in this presentation:

- SPAN/Mirror
- TAP
- Inline Bypass Switch
- Virtual

SPAN / Mirror

SPAN and Mirror are generally interchangeable terms which describe how a switch will forward a duplicate copy of passing traffic for monitoring purposes.

Pro: Mostly free.

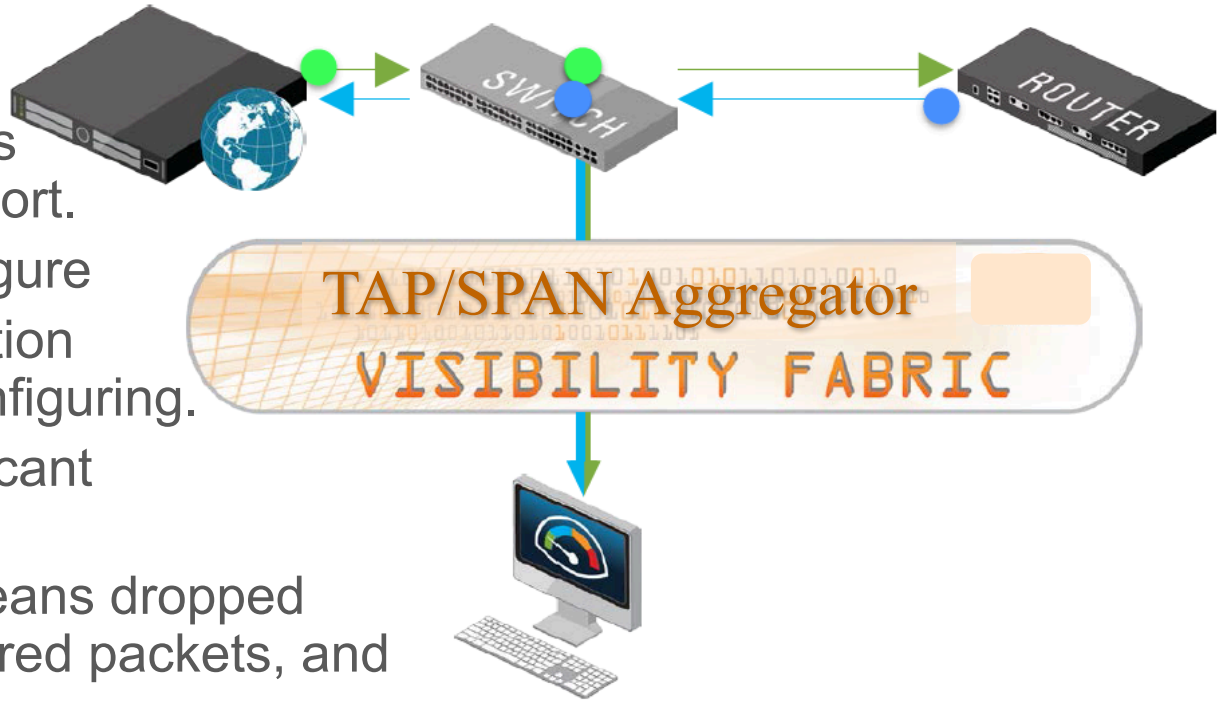
Pro: The only access for traffic port-to-port.

Pro: Easy to reconfigure

Con: Risk to production network when configuring.

Con: Slight to significant packet loss.

Con: Low priority means dropped packets, misordered packets, and timing changes.



Gigamon

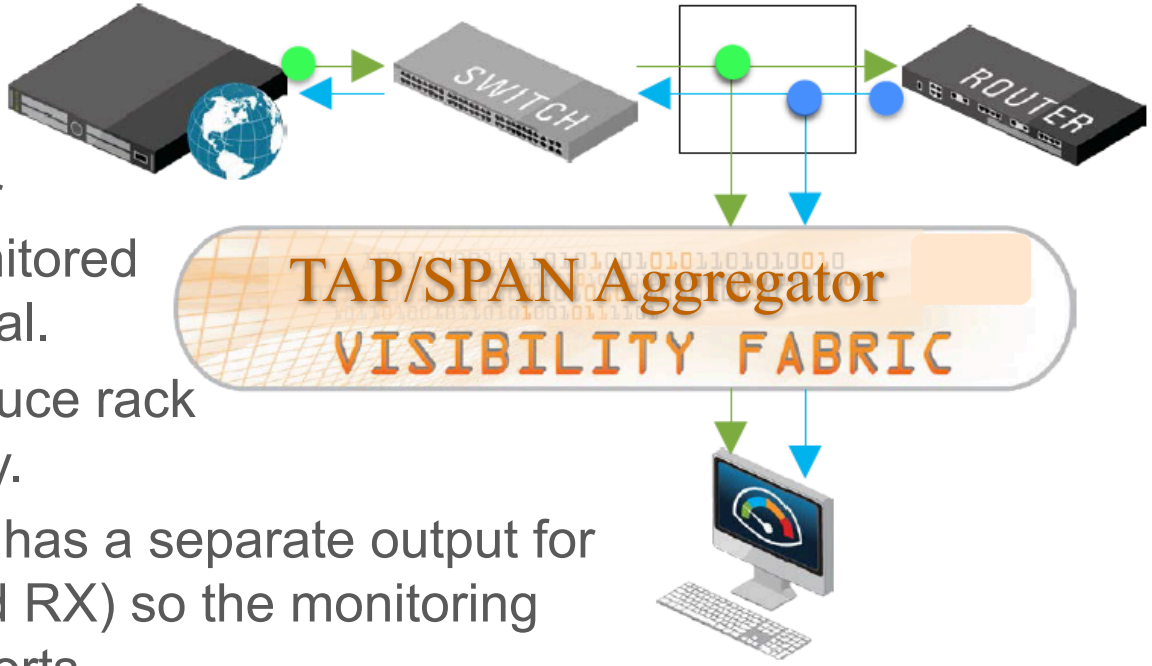
SPAN / Mirror

The effect of packet loss and other problems associated with SPAN port use:

- Higher speed SPAN ports may cause production traffic drops before monitor output traffic volume starts to approach the output link capacity.
- At 1Gb a SPAN output port can be easily oversubscribed. At 10Gb and higher speeds the switch may impose rate limiting that restricts traffic output to some percentage of the output port capacity.
- Packet reordering, latency changes, and so on may result in time spent trying to fix the wrong problem.

TAP

- TAPs are passive or active devices which offer access to all traffic flowing through the monitored link.
- Pro: A TAP is attached in series, so that all traffic must pass through it. Therefore all traffic is available.
- Pro: Most TAPs have “failsafe” protection for power loss so the monitored link remains operational.
- Pro: Internal TAPs reduce rack cabling and complexity.
- Con: A traditional TAP has a separate output for each direction (TX and RX) so the monitoring tool needs two input ports.



TAP

Using a TAP is so much better than relying on SPANs that there is a saying:

TAP where you can,

…SPAN where you must.

The one drawback relates to power loss, and the effect of power loss depends on whether the TAP is active or passive.

- Passive TAP

  Passive taps are typically unpowered so power loss to a passive TAP is nearly impossible and there would be no risk to the monitored link.

- Active TAP

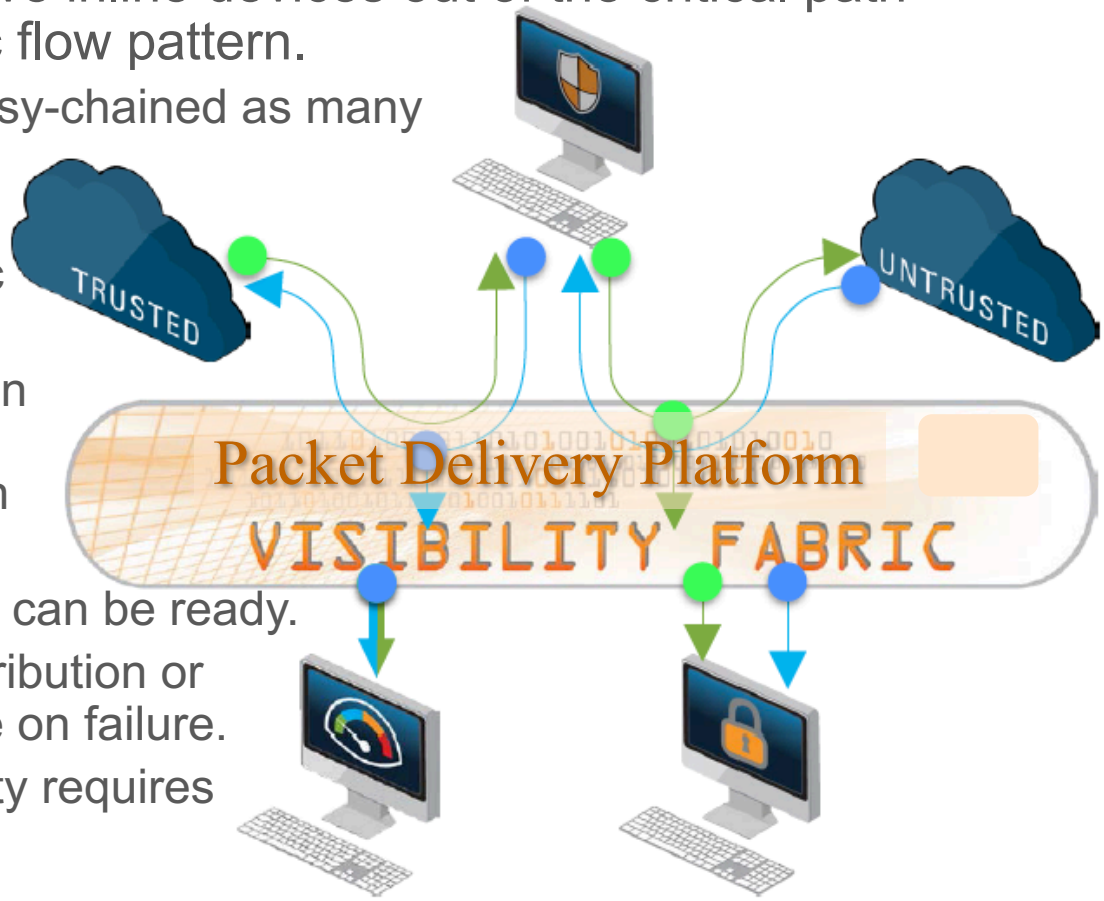
  Power loss to an active TAP may have one of two outcomes:

  - TAP is lacking “fail-safe” protection, and power loss causes the link to go down
  - TAP has “fail-safe” protection, and power loss causes a very brief interruption while Ethernet renegotiates.

Inline Bypass Switch

Inline Bypass switches move inline devices out of the critical path without changing the traffic flow pattern.

- Pro: Bypass link can be daisy-chained as many times as required.
- Pro: Automatic failure detection permits automatic removal of a failed device.
- Pro: High capacity traffic can be load-balanced to low capacity or lower bandwidth tools.
- Pro: Hot standby inline tolls can be ready.
- Pro: Automatic traffic redistribution or load balancing can be done on failure.
- Con: Increased link reliability requires additional equipment.



Gigamon

Bypass Switch

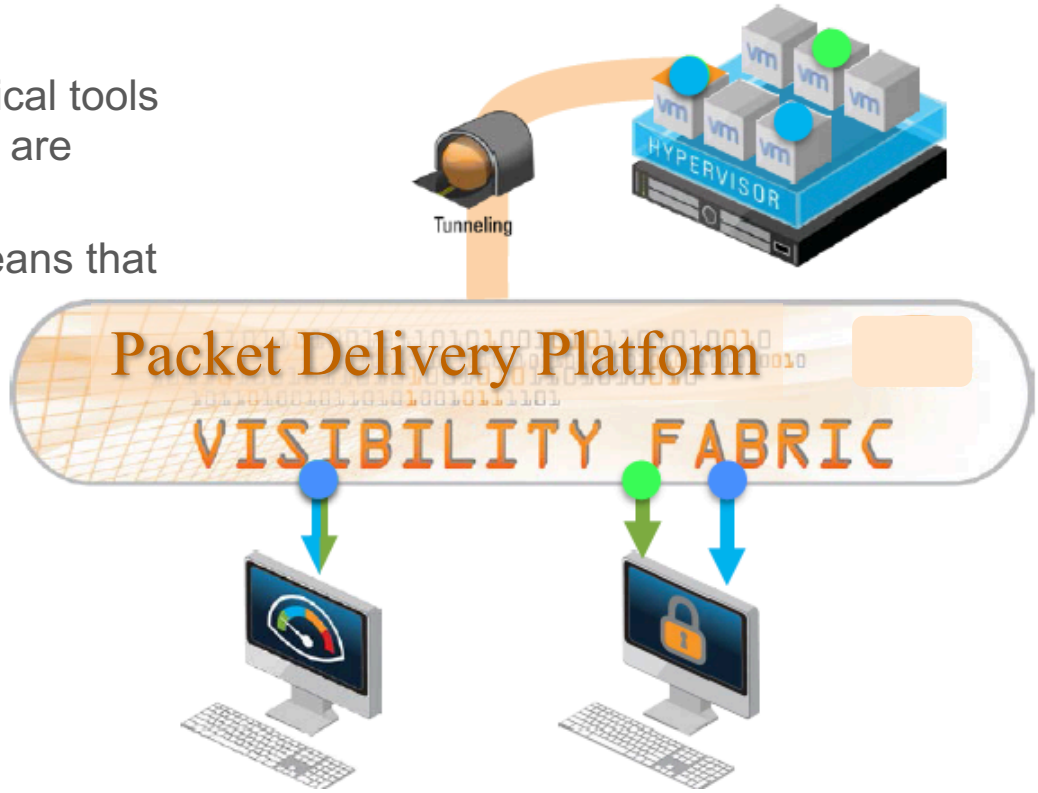
Inline devices operate just fine without a bypass switch, so why use one?

- Simultaneous inline and out-of-band traffic access
- Improved link reliability
  - Tool failure does not bring down the link
  - Tool replacement need not wait till off-hours maintenance window
  - Traffic distribution can be optimized to different tools
- Improved tool performance
  - Traffic can be load balanced across multiple like-tools
  - Safe traffic can be shunted around the inline tool
- Improved inline security
  - A standby tool can take over if the primary tool fails or need maintenance
  - Traffic can be redistributed if a tool fails or need maintenance

Virtual

Accessing traffic flowing between virtual machines requires access to packets inside each hypervisor. There are two common approaches: install duplicate tools in each hypervisor, or send traffic out to physical tools.

- Pro: Forwarding traffic out to physical tools means more hypervisor resources are available to the virtual machines.
- Pro: Forwarding traffic out also means that monitoring and security profiles are unchanged.
- Con: Forwarding traffic out means that management traffic is sharing the physical NIC bandwidth.



Gigamon

Virtual

The decision to performing analysis locally (inside the hypervisor) versus remotely (using physical tools) should be carefully considered.

- Duplicate tools installed inside each hypervisor have largely unlimited traffic access since the packet access is not limited by available (shared) physical NIC bandwidth.
- Performing deep-packet inspection for monitoring and security using the hypervisor resources limits how much of those resources are available for production network activities.
- Use of vMotion can pose challenges for continuous monitoring and security very difficult, since the monitored virtual server or application may be migrated to a different hardware or even a different data center at any time.
- Public Cloud (AWS, Azure, Google Cloud, and many others)

Choosing a Traffic Source

Choosing which traffic source is best depends upon what will be done with that traffic.

- Performance Monitoring typically discards entire transactions where one or more packets are missing.
- Security also depends on entire transactions, or it cannot accurately locate and isolate threats.
- For Performance Monitoring and Security, having too many packets can also be a problem. Duplicate packets create another sort of challenge.
- Troubleshooting is made difficult when the analyzed traffic stream is not identical to the production traffic in every way.
- Trend analysis and other statistical applications do tolerate dropped packets, and also usually do not notice misordered packets or timing changes.

Visibility is Essential

Flying Blind is not fun at All

- Visibility is essential to effectively managing your network.
- You can’t manage or protect your network from what you can’t see

Gigamon

Network Security Benefits Everyone

- Visibility into your Computing Environment is beneficial to everyone, the NetworkTeam and the Security Team.
- The Network Team should always be looking for security anomalies in their device based monitoring and should be working closely with the Security Team to investigate anything out of the ordinary
- Traffic Based tools are numerous and can provide much better analysis of the computing environment, but many of these tools are deployed sporadically or without full visibility.

Thank You

- gigamon.com/blog/author/allenhebert
- www.linkedin.com/in/allenhebert
- allen.hebert@gigamon.com
- 512-657-5449

Gigamon