Maximize Network Visibility with NetFlow Technology

Andy Wilson
Sr. Systems Engineer
awilson@lancope.com
www.lancope.com
What is NetFlow

NetFlow for the IT Organization

Security Benefits of NetFlow

A Glimpse into the Power of NetFlow
  - 10+ G Ethernet Environments
  - Virtual Environments
  - MPLS and Multi-point VPNs

Threat Detection Methodologies
What is NetFlow?

NetFlow Fields
- src and dst IP
- src and dst port
- start time
- end time
- packet count
- byte count
...

Internet

StealthWatch Flow Collector
NetFlow vs. Traditional SNMP Monitoring
Flow-based Visibility and Drill-down

Flow Table - 2,143 records

<table>
<thead>
<tr>
<th>Duration</th>
<th>Client Host</th>
<th>Server Host</th>
<th>Service Summary</th>
<th>Average Rate (bps)</th>
<th>Total Bytes</th>
<th>Total Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 minutes</td>
<td>10.201.1.123</td>
<td>10.201.1.29</td>
<td>ssh (2/tcp)</td>
<td>124.23M</td>
<td>6.07G</td>
<td>6,536,776</td>
</tr>
<tr>
<td>1s</td>
<td>10.201.0.17</td>
<td></td>
<td>Unprofiled tcp</td>
<td>4.59M</td>
<td>560.48k</td>
<td>1,166</td>
</tr>
<tr>
<td>34 minutes</td>
<td>10.201.3.35</td>
<td>smodems.lancope.com</td>
<td>(216.81.122.230)</td>
<td>518.4.0.264/tcp</td>
<td>966.43k</td>
<td>235.02k</td>
</tr>
<tr>
<td>&lt; 1s</td>
<td>218.23.37.51</td>
<td>145.179.lancope.com</td>
<td>(205.182.179.145)</td>
<td>sql-server (1434/udp)</td>
<td>749.82k</td>
<td>91.13k</td>
</tr>
<tr>
<td>&lt; 1s</td>
<td>218.23.37.51</td>
<td>209.182.189.90</td>
<td>sql-server (1434/udp)</td>
<td>749.82k</td>
<td>91.13k</td>
<td>232</td>
</tr>
<tr>
<td>&lt; 1s</td>
<td>122.225.100.154</td>
<td>209.182.189.94</td>
<td>sql-server (1434/udp)</td>
<td>743.36k</td>
<td>90.74k</td>
<td>230</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>717.5k</td>
<td>87.5k</td>
<td>222</td>
</tr>
</tbody>
</table>

Quick View for Time

©2010 Lancope, Inc.
NetFlow for the Network Team

- Interface utilization
- Billing and chargeback
- QOS monitoring
- BGP ASN monitoring
- MPLS visibility
- Application troubleshooting

NetFlow Packet
- flow1
- flow2
- ...

StealthWatch Flow Collector

Network Team:
Compliance and Auditing
Security Team
PCI Compliance
File sharing
HIPAA Compliance
Malware outbreak detection
SCADA Security
Network acceptable use
Sarbanes-Oxley
Flow forensics
Data loss prevention

©2010 Lancope, Inc.
NetFlow Compliance and Auditing

Network Team
- Interface utilization
- Billing and chargeback
- QOS monitoring
- BGP ASN monitoring
- MPLS visibility
- Application troubleshooting

Compliance and Auditing
- PCI Compliance
- HIPAA Compliance
- SCADA Security
- Sarbanes-Oxley
- RIAA & DMCS

Security Team
- File sharing
- Malware outbreak detection
- Network acceptable use
- Flow forensics
- Data loss prevention
NetFlow for the Security Team

Network Team
- Interface utilization
- Billing and chargeback
- QOS monitoring
- BGP ASN monitoring
- MPLS visibility
- Application troubleshooting

Compliance and Auditing
- PCI Compliance
- HIPAA Compliance
- SCADA Security
- Sarbanes-Oxley
- RIAA & DMCS

Security Team
- File sharing
- Malware outbreak detection
- Network acceptable use
- Flow forensics
- Data loss prevention
NetFlow Security Benefits

- Real-time monitoring of host behaviors and traffic analysis to identify internal and external threats
- Quickly pinpoint zero-day and unknown threats that bypass perimeter security
- Identify policy violations, unauthorized activity/applications, misconfigured hosts, and other rogue devices
- Monitor high-speed, highly segmented and highly meshed networks without introducing the costs and complexity associated with point solutions
- Faster Incident Resolution & detailed Forensic data
- Detection of DoS/DDoS attacks, Worms, Viruses and Botnets
- Track and Audit network behavior and access by Individual Hosts
- Detect peer-to-peer (P2P) activity
- Tie user identity to network activity
- Ensure regulatory compliance
Stay RIAA & DMCS Compliant

Demonstrates compliance with Recording Industry Association of America (RIAA) and the U.S. Digital Millennium Copyright Act (DMCA)

• Conduct IP- to-ID mapping to tie host to end users
• Alarm on high traffic hosts, including file sharing hosts, to quickly identify potential abusers of file sharing technology
• Detect anomalous behavior where network activity deviates from the norm
• Log user activity to help track both initial and subsequent infringement activities
StealthWatch allows administrators to drill down from the High File Sharing Index alarm into the user identity tab of the Host Snapshot.
Regain the Visibility Lost Due to New Technologies
Visibility Lost Due to New Technologies

New network technologies are outpacing traditional network monitoring techniques such as SNMP and SPAN/tap-based technology...

- "10G Ethernet is so fast few probe technologies can keep up and those that can are too expensive”
- "MPLS and multi-point VPNs create a meshed WAN that’s expensive to monitor adequately”
- "Virtualization hides whole network segments from the network manager’s view, making VM2VM communication problems difficult to troubleshoot”

These issues result in an inability to react to network problems because of a basic lack of *visibility*.
“10G Ethernet is so fast few probe technologies can keep up and those that can are too expensive”
NetFlow in a 10G+ Ethernet Environment

“10G Ethernet is so fast few probe technologies can keep up and those that can are extremely expensive”
“Virtualization hides whole network segments from the network manager’s view, making VM2VM communication problems difficult to troubleshoot”
NetFlow in the Virtual Environment

- Cisco Nexus 1000v also supports NetFlow

StealthWatch Flow Collector
“MPLS and multi-point VPNs create a meshed WAN that’s expensive to monitor adequately”
Fully meshed connectivity circumvents network monitoring deployed at the “hub” location…
MPLS and Multi-point VPNs

Full visibility requires a probe at each location throughout the WAN…
Deploy a StealthWatch NetFlow collector at a central location and enable NetFlow at each remote site...
Threat Detection Methodologies
### Threat Detection Method #1: Pattern Recognition

<table>
<thead>
<tr>
<th>Client Host</th>
<th>Server Host</th>
<th>Service Summary</th>
<th>Server Total Bytes</th>
<th>Client Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.214</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.212</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.216</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.206</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.210</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.208</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.213</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.200</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.209</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.206</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.211</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.213</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.113</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
</tbody>
</table>

**Anomalous Traffic Counts and Statistics**
Threat Detection Method #2: Behavior-based Analysis

Collect and analyze flows

Establish baseline of behavior
- Number of concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of Syns received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Alarm on anomalies and changes in behavior

Anomaly detected in host behavior

Critical Servers  | Exchange Servers  | Web Servers  | Marketing
1. Collect flows from network routers or a Lancope FlowSensor. Be sure to cover all major Internet uplinks.

2. For each flow elect a "client" and a "server". The client is the side that initiated the transfer.

3. Build up a baseline of the average amount of data bytes flowing from clients within your internal network to servers out on the Internet.

4. Raise alerts and build reports that describe uploads to servers on the Internet that appear to be outside the norm.

Example:
Suspect Data Loss
Threat Detection Method #3: Visualization

![Graph showing traffic and time]
Threat Detection Method #3: Visualization

Server: SMC Demo2.colo.lancope.com (216.83.162.230) from Lancope Colocation
Client: 23.30.178.230.broad.static.hf.ah.cndata.com (23.30.178.230) from China
Service: ssh
Total bytes: 12,491,776 bytes
Threat Detection Method #3: Visualization

<table>
<thead>
<tr>
<th>Average Rate (bps)</th>
<th>Client Host</th>
<th>Client Zone</th>
<th>Server Host</th>
<th>Server Zone</th>
<th>Service Summary</th>
<th>Start Active Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.01K</td>
<td>220.178.30.233</td>
<td>China</td>
<td>10.192.0.33</td>
<td>10.192.0.33</td>
<td>ssh (22/tcp)</td>
<td>Feb 12, 2009 2:39:14 AM</td>
</tr>
<tr>
<td>9.88K</td>
<td>220.178.30.233</td>
<td>China</td>
<td>10.192.0.52</td>
<td>VMWare50</td>
<td>ssh (22/tcp)</td>
<td>Feb 12, 2009 2:39:14 AM</td>
</tr>
<tr>
<td>9.74K</td>
<td>220.178.30.233</td>
<td>China</td>
<td>10.192.0.74</td>
<td>VMWare70</td>
<td>ssh (22/tcp)</td>
<td>Feb 12, 2009 2:39:14 AM</td>
</tr>
<tr>
<td>9.73K</td>
<td>220.178.30.233</td>
<td>China</td>
<td>10.192.0.51</td>
<td>VMWare50</td>
<td>ssh (22/tcp)</td>
<td>Feb 13, 2009 2:39:14 AM</td>
</tr>
</tbody>
</table>
Quick Recap: Security Operations

• **NetFlow provides**… visibility across the entire reach of an enterprise network – even across highly switched, highly segmented or fully meshed environments

• **NetFlow provides**… administrators with true, real-time feedback on the current security status anywhere on the network

• **NetFlow provides**… automatic threat mitigation to stop even unknown threats instantly

• **NetFlow provides**… actionable intelligence needed to quickly resolve network incidents
Questions?

awilson@lancope.com

sales@lancope.com