Securing and Monitoring BYOD Networks using NetFlow

How NetFlow can help with Security Analysis, Application Detection and Traffic Monitoring

Don Thomas Jacob
Technical Marketing Engineer
ManageEngine NetFlow Analyzer

ZOHO
ManageEngine is an IT management vendor focused on bringing a complete IT management portfolio to all types of enterprises.
Today’s Agenda

• What is BYOD
• Audience Poll
• Reasons for Concern
• Limitations of BYOD Solutions
• What is NetFlow
• Why NetFlow for BYOD Networks
• Questions
What is BYOD

Define: BYOD (Bring Your Own Device)

“ The practice of allowing employees to bring their own computing devices like smartphones, laptops or PDA to the workplace for use and connectivity on the corporate network. “
Define: BYOD (Bring Your Own Device)

“The practice of allowing employees to bring their own computing devices like smartphones, laptops or PDA to the workplace for use and connectivity on the corporate network.”

- **Cost Savings**
  - Device/Hardware cost transferred to employee

- **Free up your IT Team**
  - Ownership on the employee – Devices handled better
  - Reduce the time spend by IT team on end-user device support and troubleshooting

- **Employee Satisfaction**
  - Flexibility to work when & where as needed, on ones own chosen device

- **Increased Productivity**
  - Telecommuting and flexible working hours increase productivity
An Aberdeen study in July 2011 found 75% organizations are permitting BYOD for business purposes.

Gartner study says that by 2014, 90 percent of organizations will support corporate applications on personal devices.

Cisco is adopting a "Any Service, Any Device, Anywhere" architecture which will evolve to a "Virtual Enterprise" – An enterprise which is location and service independent.
POLL

What is your organization’s decision regarding BYOD implementation?

- BYOD allowed for all device types including laptops
- BYOD permitted only for smartphones/tablets
- Planning to implement
- Currently not considering
BYOD: Reasons for Concern
Reasons for Concern

Nascent Mobile Device Management (MDM)
- No established MDM policies and monitoring solutions
- No multi-platform or IPv6 support, may not be user friendly, etc.

Different devices, Different Operating Systems
- Patch management and Compliance issues

Lack of Visibility
- Where is the device in the network?
- What is it accessing?

Applications - Unverified and Untrusted
- Security issues, Malwares and Bandwidth Issues

Vanishing Network Perimeter
- Remote connections, Security concerns
Personal Work @ Work

- Tendency to use BYOD for personal purposes

- Exponential growth in HD Video and social media

- Live Streaming of highly popular NCAA men's college basketball tournament was made available on Android devices

- Non-business related traffic volume increases

BANDWIDTH Issues / Poor Business Application Performance
Device Loss = Data Loss
**Device Loss = Data Loss**

- Biggest threat is when BYOD leaves the enterprise network
- Business data / internal emails stored on device
- Device loss leads to sensitive information being left in the open
- Stolen device can be used to connect to your network remotely for data theft or attacks

**Major SECURITY Issues**
• Mobile device growth has lead to an application explosion

• New and unverified applications downloaded and installed

• Security threats and malwares risks comes along unverified apps

• Greedy Apps: Un-optimized, bandwidth hogging applications

• Bottlenecks due to traffic from junk applications

SECURITY Issues & BANDWIDTH Bottlenecks
Inviting Network Threats

• BYOD users browse from unsecured Wi-Fi networks, visits untrusted sites or download from untrusted vendors

• “Dancing pigs over Security” – Users can be careless and devices outside the network perimeter are easier to attack and infect

![Dancing pigs over Security](image1.png)

![Possible Malware alert](image2.png)
Inviting Network Threats

- BYOD users browse from unsecured Wi-Fi networks, visits untrusted sites or download from untrusted vendors.

- “Dancing pigs over Security” – Users can be careless and devices outside the network perimeter are easier to attack and infect.

- Huge increase in number of malwares targeting mobile software platforms like iOS and Android.

- Infected device carried into the network – Malware enters LAN.

Network open to **MALWARE**
Limitations of BYOD Solutions
Limitations of BYOD Solutions

More Control on BYOD Devices & Web Traffic

**Limitation:** As good as having company issued device - BYOD advantage lost
Vague and impractical solution - Genuine users will be effected

Up-to-date Patch Management

**Limitation:** No multi-platform MDM or patch management solution available for the highly diverse mobile ecosystem

Anti-Virus Software on Mobile Devices

**Limitation:** New age malware exploits zero-day vulnerabilities

Multi Layered Security & Internal IDS

**Limitations:** Traditional, layered security solutions (firewall, proxy, content filtering, etc.) will fall short against new age threats
Expensive to implement IDS/IPS in access layer to stop internal malware
What is NetFlow
What is NetFlow

Technology developed by Cisco - Designed as a switching path

Is now the **Primary IP Traffic** accounting technology

Information on the WHO, WHAT, WHEN and WHERE of IP traffic

All major vendors now support flow export:

- **NetFlow** - Cisco, Adtran, 3COM
- **J-Flow** - Juniper
- **IPFIX** - Nortel
- **sFlow** - Alcatel, HP, Brocade, Enterasys, Dell
What is NetFlow

7 unique fields define a flow

- Source Interface (ifindex)
- Protocol
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- ToS
How NetFlow Works

- Traffic passes through routing/switching device interface
- Flow created (remember the 7 fields) and stored in NetFlow cache
- Flows grouped and exported in UDP packets to collector based on active and inactive flow timeout
What is NetFlow

- NetFlow enabled interface
- NetFlow Packets
  - Approximately 1500 bytes
  - Each contains 20-50 flow records

NetFlow Collector

Core Network

Edge Router

UDP NetFlow
What is NetFlow

- **Who?**
  - Source IP Address
  - Destination IP Address

- **When?**
  - Flow Start and End time

- **What?**
  - Source Port
  - Destination Port
  - Protocol
  - Packet Count
  - Octet count

- **Usage?**
  - QoS
  - TCP Flags
  - Protocol

- **Path?**
  - Input and Output Interface (ifindex)

- **Route?**
  - NextHop
  - Source AS Information
  - Destination AS Information

Who?

What?

Usage?

Route?

Path?

When?

What?
Why NetFlow for BYOD Networks
In-Depth Tracking

- NetFlow provides real-time information about network traffic
- BYOD monitoring begins at the access layer - Closer to traffic source
In-Depth Tracking

- NetFlow provides real-time information about network traffic
- BYOD monitoring begins at the access layer - Closer to traffic source
- Flow export supported on most enterprise devices including core and access layer switches
- No impact on the network and devices due to flow export
In-Depth Tracking

- NetFlow provides real-time information about network traffic
- BYOD monitoring begins at the access layer - Closer to traffic source
- Flow export supported on most enterprise devices including core and access layer switches
- No impact on the network and devices due to flow export
- Track impact of BYOD on bandwidth, who are the top talkers for each interface and IP Subnet
- What are the devices doing on your network, what application is being used and what is the destination of traffic
NetFlow provides real-time information about network traffic. BYOD monitoring begins at the access layer, closer to the traffic source. Flow export is supported on most enterprise devices, including core and access layer switches. There is no impact on the network and devices due to flow export. Track the impact of BYOD on bandwidth, who are the top talkers for each interface and IP Subnet. What are the devices doing on your network, what application is being used, and what is the destination of traffic?

Why NetFlow for BYOD

In-Depth Tracking

<table>
<thead>
<tr>
<th>Category</th>
<th>Total</th>
<th>Min</th>
<th>Max</th>
<th>Avg</th>
<th>Standard Deviation</th>
<th>95th Percentile</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN</td>
<td>234.61 GB</td>
<td>1.31 Mbps</td>
<td>73.62 Mbps</td>
<td>12.12 Mbps</td>
<td>11.87 Mbps</td>
<td>35.31 Mbps</td>
</tr>
<tr>
<td>OUT</td>
<td>46.61 GB</td>
<td>2.4 Mbps</td>
<td>24.4 Mbps</td>
<td>2.98 Mbps</td>
<td>7.4 Mbps</td>
<td></td>
</tr>
</tbody>
</table>

Traffic IN Details

<table>
<thead>
<tr>
<th>Time</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-25-12 21:00</td>
<td>11.00 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 20:00</td>
<td>17.27 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 19:00</td>
<td>27.62 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 18:00</td>
<td>40.50 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 17:00</td>
<td>32.4 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 16:00</td>
<td>32.07 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 15:00</td>
<td>35.47 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 14:00</td>
<td>35.31 Mbps</td>
</tr>
</tbody>
</table>

Traffic OUT Details

<table>
<thead>
<tr>
<th>Time</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-25-12 21:00</td>
<td>3.24 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 20:00</td>
<td>4.02 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 19:00</td>
<td>5.99 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 18:00</td>
<td>6.56 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 17:00</td>
<td>6.2 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 16:00</td>
<td>6.17 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 15:00</td>
<td>6.75 Mbps</td>
</tr>
<tr>
<td>Jun-25-12 14:00</td>
<td>7.4 Mbps</td>
</tr>
</tbody>
</table>
Why NetFlow for BYOD

In-Depth Tracking

- NetFlow provides real-time information about network traffic.
- BYOD monitoring begins at the access layer, closer to traffic source.
- Flow export supported on most enterprise devices including core and access layer switches.
- No impact on the network and devices due to flow export.
- Track impact of BYOD on bandwidth, who are the top talkers for each interface and IP Subnet.
- What are the devices doing on your network, what application is being used and what is the destination of traffic.

In-Depth Tracking:

Top Traffic - Source IN

172.18.2.205 [ffindex2]
Why NetFlow for BYOD

In-Depth Tracking

NetFlow provides real-time information about network traffic.

BYOD monitoring begins at the access layer—closer to traffic source.

Flow export supported on most enterprise devices including core and access layer switches.

No impact on the network and devices due to flow export.

Track impact of BYOD on bandwidth, who are the top talkers for each interface and IP Subnet.

What are the devices doing on your network, what application is being used and what is the destination of traffic.

In-Depth Tracking
Why NetFlow for BYOD

Where is the Network Perimeter

- Vanishing network perimeter
- Increase in telecommuting and hence more remote connections with BYOD
- Stolen mobile devices or malware infected devices can be used to connect to the enterprise network over VPN
- Flow export supported by all major firewalls and routers
- Use NetFlow data to see which device is connecting over tunnels and where the traffic is headed
Where is the Network Perimeter

- Vanishing network perimeter – Increase in telecommuting and hence more remote connections with BYOD

- Stolen mobile devices or malware infected devices can be used to connect to the enterprise network over VPN

- Flow export supported by all major firewalls and routers

- Use NetFlow data to see which device is connecting over tunnels and where the traffic is headed
Vanishing network perimeter

- Increase in telecommuting and hence more remote connections with BYOD
- Stolen mobile devices or malware infected devices can be used to connect to the enterprise network over VPN
- Flow export supported by all major firewalls and routers
- Use NetFlow data to see which device is connecting over tunnels and where the traffic is headed

### Why NetFlow for BYOD

#### Where is the Network Perimeter

<table>
<thead>
<tr>
<th>Application</th>
<th>Traffic (Total: 154.54 MB)</th>
<th>% of total traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown_App</td>
<td>70.97 MB</td>
<td>46%</td>
</tr>
<tr>
<td>ESP Traffic</td>
<td>25.11 MB</td>
<td>16%</td>
</tr>
<tr>
<td>GRE</td>
<td>16.3 MB</td>
<td>11%</td>
</tr>
<tr>
<td>icmp</td>
<td>7.97 MB</td>
<td>5%</td>
</tr>
<tr>
<td>sspd</td>
<td>6.87 MB</td>
<td>4%</td>
</tr>
<tr>
<td>mdns</td>
<td>6.36 MB</td>
<td>4%</td>
</tr>
<tr>
<td>bootps</td>
<td>4.79 MB</td>
<td>3%</td>
</tr>
<tr>
<td>netbios-dgm</td>
<td>4.7 MB</td>
<td>3%</td>
</tr>
<tr>
<td>llmnr</td>
<td>3.07 MB</td>
<td>2%</td>
</tr>
<tr>
<td>cslistener</td>
<td>1.84 MB</td>
<td>1%</td>
</tr>
</tbody>
</table>
New-Age Malwares

- BYOD growth = Increase in malwares targeting mobile devices
- Most new malwares are zero day based - No signature for IDS or IPS to identify and stop the malwares
- Infected devices are sometimes physically carried into the network after being infected from elsewhere
- IDS and IPS in the internal network is not feasible due to costs
- Network traffic behavior analysis can help with anomaly detection
BYOD growth = Increase in malwares targeting mobile devices

Most new malwares are zero day based - No signature for IDS or IPS to identify and stop the malwares

Infected devices are sometimes physically carried into the network after being infected from elsewhere

IDS and IPS in the internal network is not feasible due to costs

Network traffic behavior analysis can help with anomaly detection

New-Age Malwares

McAfee’s Q3 2011 Threats report shows Android operating system became the exclusive target for all new mobile malware

The amount of malware targeted at Android devices jumped more than 37% since last quarter to become the most attacked mobile operating system, and puts 2011 on track to be the busiest in mobile and general malware history.

**Source:** McAfee

*Includes variants identified after the publishing of McAfee’s Q2 Threat Report*
Why NetFlow for BYOD

New-Age Malwares

• NetFlow packets holds granular information on IP traffic behavior

• ManageEngine NetFlow Analyzer’s has Advanced Security Analytics Module (ASAM)

• ASAM leverages on the already exported NetFlow or sFlow data for behavior anomaly detection

• Real time threat detection using Continuous Stream Mining Engine technology

• Threats that surpass your IDS and other traditional security systems can be detected

• Anomaly classification based on Offender, Target, Path and Problem
Why NetFlow for BYOD

New-Age Malwares
## New-Age Malwares

### Report Details

<table>
<thead>
<tr>
<th>ID</th>
<th>Problem</th>
<th>Offender(s)</th>
<th>Routed via</th>
<th>Target(s)</th>
<th>Time</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>13678</td>
<td>Scans / Probes - Empty TCP Diagonal Scan</td>
<td>NA</td>
<td>1: [192.168.1.16]</td>
<td>NA</td>
<td>2011-07-29</td>
<td></td>
</tr>
<tr>
<td>13674</td>
<td>Scans / Probes - Empty TCP Diagonal Scan</td>
<td>NA</td>
<td>1: [192.168.1.132]</td>
<td>NA</td>
<td>2011-07-29</td>
<td></td>
</tr>
<tr>
<td>13673</td>
<td>Scans / Probes - Empty TCP Diagonal Scan</td>
<td>NA</td>
<td>1: [192.168.1.150]</td>
<td>NA</td>
<td>2011-07-29</td>
<td></td>
</tr>
</tbody>
</table>

### Why NetFlow for BYOD

NetFlow is a protocol for passively monitoring network traffic. It provides detailed information about network flows, which is useful for detecting and responding to malicious activity in BYOD environments.

### New-Age Malwares

New-Age Malwares refer to a new generation of malware that exploit vulnerabilities in modern networks, often targeting BYOD devices. These malwares can bypass traditional security measures and require advanced detection methods like NetFlow for effective monitoring.

---

**Note:** The table above is a snapshot of network flow data, showing various scans and probes with their associated IP addresses and timestamps. This data is crucial for understanding and mitigating new-age malwares in BYOD environments.
### New-Age Malwares

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>3.57 KB</td>
</tr>
<tr>
<td>Packets</td>
<td>85</td>
</tr>
<tr>
<td>Hits</td>
<td>85</td>
</tr>
<tr>
<td>Unique Source IPs</td>
<td>10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237,</td>
</tr>
<tr>
<td></td>
<td>192.168.4.239, 192.168.4.240, 192.168.4.241, 192.168.4.242, 192.168.4.243]</td>
</tr>
<tr>
<td>Unique Destination IPs</td>
<td>1: [192.168.6.93]</td>
</tr>
<tr>
<td>Unique Source Networks</td>
<td>1: [192.168.4.0/24]</td>
</tr>
<tr>
<td>Unique Destination Networks</td>
<td>1: [192.168.6.0/24]</td>
</tr>
<tr>
<td>Unique Source Ports</td>
<td>85: [11, 12, 13, 14, 15, 16, 18, 19, 20, 22, 23, 25, 26, 27, 28,</td>
</tr>
<tr>
<td></td>
<td>29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 41, 42, 43, 45, 46, 47, 48,</td>
</tr>
<tr>
<td></td>
<td>49, 50, 51, 52, 53, 54, 56, 57, 59, 60, 61, 62, 63, 64, 65, 68, 69,</td>
</tr>
<tr>
<td></td>
<td>70, 72, 73, 74, 75, 77, 78, 79, 80, 81, 82, 83, 85,...</td>
</tr>
<tr>
<td>Unique Destination Ports</td>
<td>85: [211, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223,</td>
</tr>
<tr>
<td></td>
<td>224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236,</td>
</tr>
<tr>
<td></td>
<td>237, 239, 240, 241, 243, 245, 246, 247, 248, 249, 250, 251, 252,</td>
</tr>
<tr>
<td></td>
<td>253, 254, 256, 258, 259, 261, 262, 263, 264, 265, 267, 2...</td>
</tr>
<tr>
<td>Unique Applications</td>
<td>79: [systat, daytime, msp, chargen, ftp-data, ssh, telnet, smtp,</td>
</tr>
<tr>
<td></td>
<td>nsfw-fe, msg-icp, msg-auth, ds, lep, rl, ipl, graphics, name,</td>
</tr>
<tr>
<td></td>
<td>nicname, mpm, mpm-snd, ni-ftp, audit,</td>
</tr>
<tr>
<td></td>
<td>tacacs, re-mail-ck, la-maint, xns-time, domain, xns-ch,</td>
</tr>
<tr>
<td></td>
<td>xns-auth, ni-mail, acas, whois++, ...</td>
</tr>
<tr>
<td>Unique TCP Flags</td>
<td>1: [A,R_]</td>
</tr>
<tr>
<td>Unique Protocols</td>
<td>1: [TCP]</td>
</tr>
<tr>
<td>Unique ToS Values</td>
<td>1: [2]</td>
</tr>
<tr>
<td>Unique In Interfaces (Routed Via)</td>
<td>[Cisco ASR (IfIndex2)]</td>
</tr>
<tr>
<td>Unique Out Interfaces</td>
<td>1: [Cisco ASR (IfIndex4)]</td>
</tr>
<tr>
<td></td>
<td>192.168.6.93-227,TCP: 192.168.4.234-74--192.168.6.93-237,TCP:</td>
</tr>
<tr>
<td></td>
<td>192.168.4.234-75--192.168.6.93-247,TCP: 192.168.4.234-77--192.168.6.93-</td>
</tr>
<tr>
<td></td>
<td>267,TCP: 192.168.4.234-78--192.168.6.93-277,TCP: 192.1...</td>
</tr>
<tr>
<td>Unique Router IPs</td>
<td>1 Router(s)</td>
</tr>
<tr>
<td></td>
<td>- [Cisco ASR (127.0.0.1)]</td>
</tr>
</tbody>
</table>
Conclusion

• **MDM is Evolving – Hold the high-cost investment**
  - Not multi-platform - Apple, Android, Blackberry, Symbian
  - Support for new technologies - IPv6, mobile apps
  - Many solutions are basic - Need to evolve a lot more

• **Security and monitoring most important aspects of BYOD**

• **Leverage on default or low cost technologies like NetFlow**

• **Most Important - Educate users**
  - Why security is more important than the fancy screensaver
  - Why bandwidth is important for the organization
Questions?

ManageEngine NetFlow Analyzer is used by over 4000 customers worldwide

www.netflowanalyzer.com

NetFlow Analyzer Blogs:
https://blogs.netflowanalyzer.com

User Forums:
http://forums.netflowanalyzer.com

LinkedIn:
http://www.linkedin.com/groups?gid=4208806&trk=hb_side_g

TAC Team:
etflowanalyzer-support@manageengine.com

ManageEngine Sales:
sales@manageengine.com