CISCO IOS NETFLOW AND SECURITY

INTERNET TECHNOLOGIES DIVISION

FEBRUARY 2005
Cisco IOS NetFlow

- NetFlow is a standard for acquiring IP network and operational data
- Benefits
  - Understand the impact of network changes and services
  - Improve network usage and application performance
  - Reduce IP service and application costs
  - Optimize network costs
  - Detect and classify security incidents
Network Availability Threats

Evolution of Network Availability Threats
Source: Arbor Networks

FEB 2000
Amazon, CNN, Yahoo!, EBay and ETrade downed by DDoS attacks

JAN 2001
Several of the Web’s largest sites taken down by DDoS attacks targeting a router

JAN 2002
European service provider Cloud Nine closes due to DDoS-related losses

FEB 2002
Widespread multi-vendor SNMP vulnerabilities create basis for router compromise

OCT 2002
DDoS attacks on root DNS servers

JAN 2003
SQL worm halts Internet traffic worldwide

1999
Researchers discuss DoS attacks
DoS attack tools emerge

2000
Advent of mainstream DDoS attacks

2001
Researchers discuss infrastructure attacks

2002
Infrastructure attacks emerge

2003

EVENTS

ATTACK SOURCE

TARGET

LOCAL IMPACT

GLOBAL IMPACT

COMPUTERS

NETWORK

INTERNET

COMPUTERS

INFRASTRUCTURE

Cisco.com
NetFlow Origination

- Developed by Darren Kerr and Barry Bruins at Cisco Systems in 1996
  
  US Patent 6,243,667
- The value of information in the cache was a secondary discovery
  
  Initially designed as a switching path
- NetFlow is now the *primary network accounting technology in the industry*
- NetFlow is the *emergent standard traffic engineering/capacity planning technology*
- NetFlow is the *primary network anomaly-detection technology*
- Answers questions regarding IP traffic:
  
  *Who?  What?  Where?  When?  How?* (i.e.: traffic analysis)
Key Concept - NetFlow Scalability

- Packet capture is like a wiretap
- NetFlow is like a phone bill
- This level of granularity allows NetFlow to scale for very large amounts of traffic
- A lot can be learned from a phone bill
  - Who is talking to whom
  - Over what protocols and ports
  - For how long
  - At what speed
  - For what duration
- NetFlow is a form of telemetry pushed from the routers/switches
  - Each one can be a sensor
Flow is Defined by Seven Unique Keys

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- Type of Service (ToS) byte (Differentiated Services Code Point (DSCP))
- Input logical interface (ifIndex)
## NetFlow Cache Example

### 1. Create and update flows in NetFlow cache

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIpAddr</th>
<th>DestIf</th>
<th>DestIpAddr</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>Pkts</th>
<th>SrcPort</th>
<th>SrcMsk</th>
<th>SrcAS</th>
<th>DstPort</th>
<th>DstMsk</th>
<th>DstAS</th>
<th>NextHop</th>
<th>Bytes/Pkt</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.100.21.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>11000</td>
<td>00A2</td>
<td>/24</td>
<td>5</td>
<td>00A2</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1528</td>
<td>1745</td>
<td>4</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.3.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2491</td>
<td>15</td>
<td>/26</td>
<td>196</td>
<td>15</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>740</td>
<td>41.5</td>
<td>1</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.20.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>10000</td>
<td>00A1</td>
<td>/24</td>
<td>180</td>
<td>00A1</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1428</td>
<td>1145.5</td>
<td>3</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.6.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2210</td>
<td>19</td>
<td>/30</td>
<td>180</td>
<td>19</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1040</td>
<td>24.5</td>
<td>14</td>
</tr>
</tbody>
</table>

### 2. Expiration

- Inactive timer is expired (15 sec is default)
- Active timer is expired (30 min (1800 sec) is default)
- NetFlow cache is full (oldest flows are expired)
- RST or FIN TCP flag

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIpAddr</th>
<th>DestIf</th>
<th>DestIpAddr</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>Pkts</th>
<th>SrcPort</th>
<th>SrcMsk</th>
<th>SrcAS</th>
<th>DstPort</th>
<th>DstMsk</th>
<th>DstAS</th>
<th>NextHop</th>
<th>Bytes/Pkt</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.100.21.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>11000</td>
<td>00A2</td>
<td>/24</td>
<td>5</td>
<td>00A2</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1528</td>
<td>1800</td>
<td>4</td>
</tr>
</tbody>
</table>

### 3. Aggregation

- **Yes**

### 4. Export version

- **Non-Aggregated Flows**—Export Version 5 or 9

### 5. Transport protocol

- **Header**: Export Packet
- **Payload (Flows)**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Pkts</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Bytes/Pkt</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>11000</td>
<td>00A2</td>
<td>00A2</td>
<td>1528</td>
</tr>
</tbody>
</table>

**Aggregated Flows**—Export Version 8 or 9
What is an Anomaly?

• An event or condition in the network that is identified as a statistical abnormality when compared to typical traffic patterns gleaned from previously collected profiles and baselines

• NetFlow allows the user to identify anomalies by producing detailed accounting of traffic flows
NetFlow is Useful for Security

- High level diagnostics to classify and identify network anomalies

- NetFlow mitigates attacks
  - Identify the attack
    - Changes in network behaviour are obvious with NetFlow
  - Classify the attack
    - Small size flows to same destination
    - Detailed flow information who, what, when, and where
      - What is being attacked and origination of attack
      - How long the attack is taking place
      - Size of packets used in the attack

- NetFlow Security partners Arbor Networks, Protego, Mazu, Adlex
Detecting DoS Attacks with Netflow

- Changes or number of flows count signify an attack

On border routers, every X min:

Count flows with sampling 1/Y during Z sec

If # of flows > N, Alarm!

DANTE uses:
X=15 min, Y=200, Z=10 sec, N=10

Values are empirical
How Does a DoS Attack Look Like?

Potential DoS attack (33 flows) on router1
Estimated: 660 pkt/s  0.2112 Mbps
ASxxx is: ...
ASddd is: ...

<table>
<thead>
<tr>
<th>src_ip</th>
<th>dst_ip</th>
<th>in_int</th>
<th>out_int</th>
<th>src_port</th>
<th>dest_port</th>
<th>pkts</th>
<th>bytes</th>
<th>prot</th>
<th>src_as</th>
<th>dst_as</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.xx.xxx.69</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1308</td>
<td>77</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.222</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1774</td>
<td>1243</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.108</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1869</td>
<td>1076</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.159</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1050</td>
<td>903</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.54</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>2018</td>
<td>730</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.136</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1821</td>
<td>559</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.216</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1516</td>
<td>383</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.111</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1894</td>
<td>45</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.29</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1600</td>
<td>1209</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.24</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1120</td>
<td>1034</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.39</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1459</td>
<td>868</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.249</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1967</td>
<td>692</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
<tr>
<td>192.xx.xxx.57</td>
<td>194.yyy.yyy.2</td>
<td>29</td>
<td>49</td>
<td>1044</td>
<td>521</td>
<td>1</td>
<td>40</td>
<td>6</td>
<td>xxx</td>
<td>ddd</td>
</tr>
</tbody>
</table>

... ...

How Does a DoS Attack Look Like?

Potential DoS attack (33 flows) on router1
Estimated: 660 pkt/s  0.2112 Mbps
ASxxx is: ...
ASddd is: ...

Real data deleted in this presentation
Tracing Back with Netflow

- Routers need Netflow to be enabled

```
router1#sh ip cache flow | include <destination>
Se1 <source> Et0 <destination> 11 0013 0007 159
.... (lots more flows to the same destination)
```

The flows come from serial 1

```
router1#sh ip cef se1
Prefix         Next Hop         Interface
0.0.0.0/0       10.10.10.2       Serial1
10.10.10.0/30   attached         Serial1
```

Find the upstream router on serial 1

Continue on this router
show ip cache flow

```
router_A#sh ip cache flow
IP packet size distribution (85435 total packets):
  1-32  64   96  128  160  192  224  256  288  320  352  384  416  448  480
     .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
     .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2728 active, 1368 inactive, 85310 added
  463824 agent polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
last clearing of statistics never

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Packets/Sec</th>
<th>Bytes/Pkt</th>
<th>Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-X</td>
<td>2</td>
<td>0.0</td>
<td>1440</td>
<td>0.0</td>
<td>9.5</td>
</tr>
<tr>
<td>TCP-other</td>
<td>82580</td>
<td>11.2</td>
<td>1440</td>
<td>11.2</td>
<td>12.0</td>
</tr>
<tr>
<td>Total</td>
<td>82582</td>
<td>11.2</td>
<td>1440</td>
<td>11.2</td>
<td>12.0</td>
</tr>
</tbody>
</table>

SrcIf         SrcIPaddress          DstIf         DstIPaddress          Pr SrcP DstP Pkts
Et0/0         132.122.25.60        Se0/0         192.168.1.1           06 9AAE 0007 1
Et0/0         139.57.220.28        Se0/0         192.168.1.1           06 708D 0007 1
Et0/0         165.172.153.65       Se0/0         192.168.1.1           06 CB46 0007 1
```
show ip cache verbose flow

text output:

```
router_A#sh ip cache verbose flow
IP packet size distribution (23597 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
    .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1323 active, 2773 inactive, 23533 added
  151644 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Flows /Sec</th>
<th>Packets /Flow</th>
<th>Bytes /Pkt</th>
<th>Packets Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-other</td>
<td>22210</td>
<td>3.1</td>
<td>1</td>
<td>1440</td>
<td>3.1</td>
<td>0.0</td>
</tr>
<tr>
<td>Total:</td>
<td>22210</td>
<td>3.1</td>
<td>1</td>
<td>1440</td>
<td>3.1</td>
<td>0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>Dst IPaddress</th>
<th>Pr</th>
<th>TOS</th>
<th>Flgs</th>
<th>Pkts</th>
<th>Port</th>
<th>Msk</th>
<th>AS</th>
<th></th>
<th>Port</th>
<th>Msk</th>
<th>AS</th>
<th>NextHop</th>
<th>B/Pk</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>216.120.112.114</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>00</td>
<td>10</td>
<td>1440</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5FA7 /0</td>
<td>0007 /0</td>
<td>0000 /0</td>
<td>0.0.0.0</td>
<td>1440</td>
<td>0.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/0</td>
<td>175.182.253.65</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>00</td>
<td>10</td>
<td>1440</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Internet and Security Benefits

- Avoidance of SQL Slammer Worm

  On January 24, 2003, the SQL Slammer worm, also called Sapphire, propagated worldwide in just eight minutes. Networks fell worldwide, including entire networks of automated teller machines and leading enterprises.

- Cisco experienced no loss of business continuity from SQL Slammer

  IT team attributes the victory to a teamwork, an established communications plan, a robust network architecture, and the effective use of Cisco IOS NetFlow technology.
DoS Attacks and Other Undesirable Traffic

- Cisco IT uses NetFlow data to protect the network from viruses and attacks and to understand the effects of current and planned applications on the network.

- From time to time Cisco receives traffic intended to produce a DoS attack.

  DoS attacks flood the network with packets, often of an unusual size, from an untrusted source to a single destination.

- Cisco detects and prevents DoS attacks by using Cisco IOS NetFlow to collect:

  - Packet source
  - Port number
  - Destination
  - Packet size
  - Protocol number

- Collected information is sent to Arbor Peakflow DoS for anomaly detection.
1. Profile: base line traffic patterns in the network
2. Monitor: analyze traffic for anomalies
3. Detect: forward anomaly fingerprints to controllers
4. Trace: trace the attack to its source
5. Filter: recommend filters (X)
NetFlow-Based Traffic Characterization
Arbor

Anomaly 10229 Information

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Severity</th>
<th>Duration</th>
<th>Direction</th>
<th>Resource</th>
<th>Start Time</th>
<th>End Time</th>
<th>Class</th>
<th>Subclass</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10229</td>
<td>High</td>
<td>5,284.9% of 275 pps</td>
<td>1h 42m 46s</td>
<td>Incoming</td>
<td>61.152.23.174/32</td>
<td>21:19:55 GMT 16 Feb 2003</td>
<td>23:02:41 GMT 16 Feb 2003</td>
<td>Misuse</td>
<td>TCP SYN Flag Anomaly</td>
<td></td>
</tr>
</tbody>
</table>

Affected Network Elements
Router bur-brdr-01 (205.171.0.122)

<table>
<thead>
<tr>
<th>Bitrate</th>
<th>Triggering</th>
<th>Expected</th>
<th>Difference</th>
<th>Maximum</th>
<th>Mean</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Rate</td>
<td>14.66 Kpps</td>
<td>3.00 Kpps</td>
<td>11.66 Kpps</td>
<td>4.56 Mbps @ 21:29</td>
<td>3.72 Mbps</td>
<td></td>
</tr>
</tbody>
</table>

Interface 23 POS7/1 (OC12 to Sprint; CORE# 27221039; MFS ckt o3-owb-bgjf-0001; TBS ckt)

<table>
<thead>
<tr>
<th>Bitrate</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.72 Mbps @ 21:24</td>
<td>2.95 Mbps</td>
</tr>
</tbody>
</table>
Protego Networks Tracing Attack

Incident Graph-245738986

Session ID:
S:266156411

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:
ICMP Ping Network Sweep

Session ID:
S:266156412

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:
ICMP Ping Network Sweep

Session ID:
S:266156461

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:
WWW IIS .ida Indexing
Service Overflow

Session ID:
S:266167384

www.protegonetworks.com
**NetFlow MIB**

- Currently available in Cisco IOS® Software Releases 12.3(7)T
- NetFlow information is available:
  - When using SNMP
  - Without NetFlow export
- Administration of Netflow using the MIB interface
- NetFlow MIB cannot be used to retrieve all Flow information, but is very useful for security monitoring and locations where export is not possible
  - Packet size distribution
  - Number of bytes exported per second
  - Number of NetFlow MIB flows with Export of Top N talkers
- **Top N Talkers**
  - Top N Flows are based on various NetFlow field values (AS Number, destination, ports)
  - MIB and CLI support
  - Releases 12.2(25)S and 12.3(11)T
Import Flow Mask Filters

- Prevent flows from entering NetFlow cache by using Flow Filter
- Useful during security or attack circumstances to isolate an attack and decrease CPU hit from router
- Increase scalability and decrease CPU usage
- Filters are based on Modular Quality of Service (QoS) Command Line Interface (CLI) (MQC) class maps
- User can use Access Control List (ACL) to match flows from certain port or source
- Define Traffic Class (match ACL) and Flow Sampling per Match

Traffic Filter

- High Importance: Sample 1:1 from Server B
- Low Importance: Sample 1:100 from Subnet A
References

• www.cisco.com/go/netflow