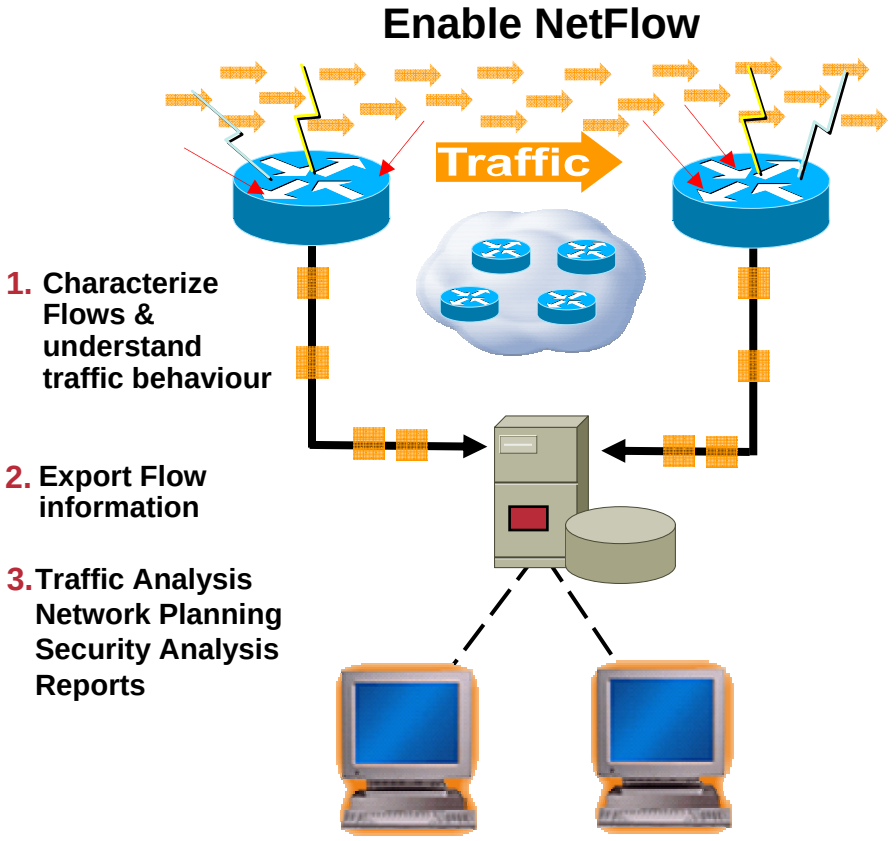
CISCO IOS NETFLOW AND SECURITY

INTERNET TECHNOLOGIES DIVISION

FEBRUARY 2005

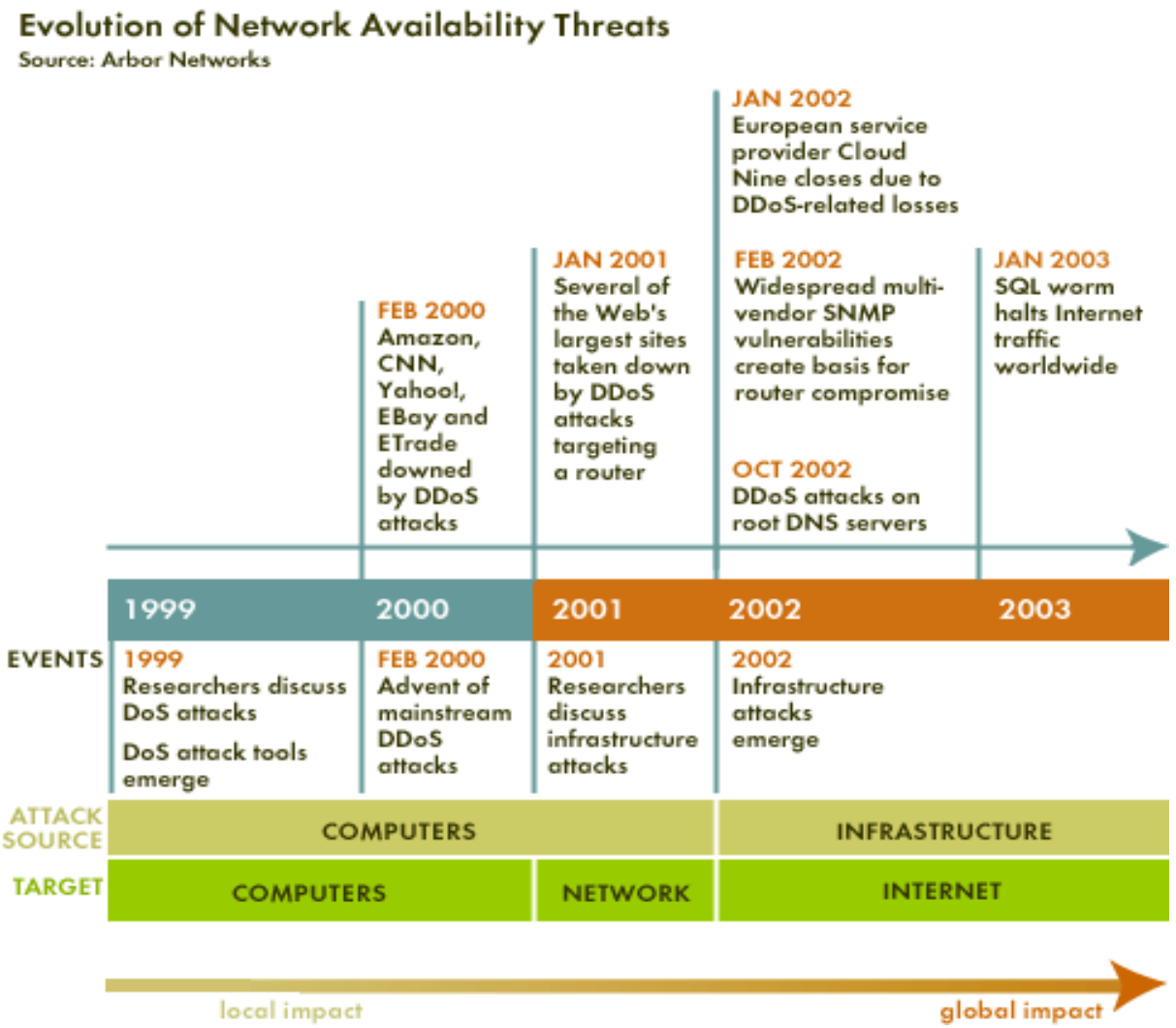
Cisco IOS NetFlow

- 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

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)

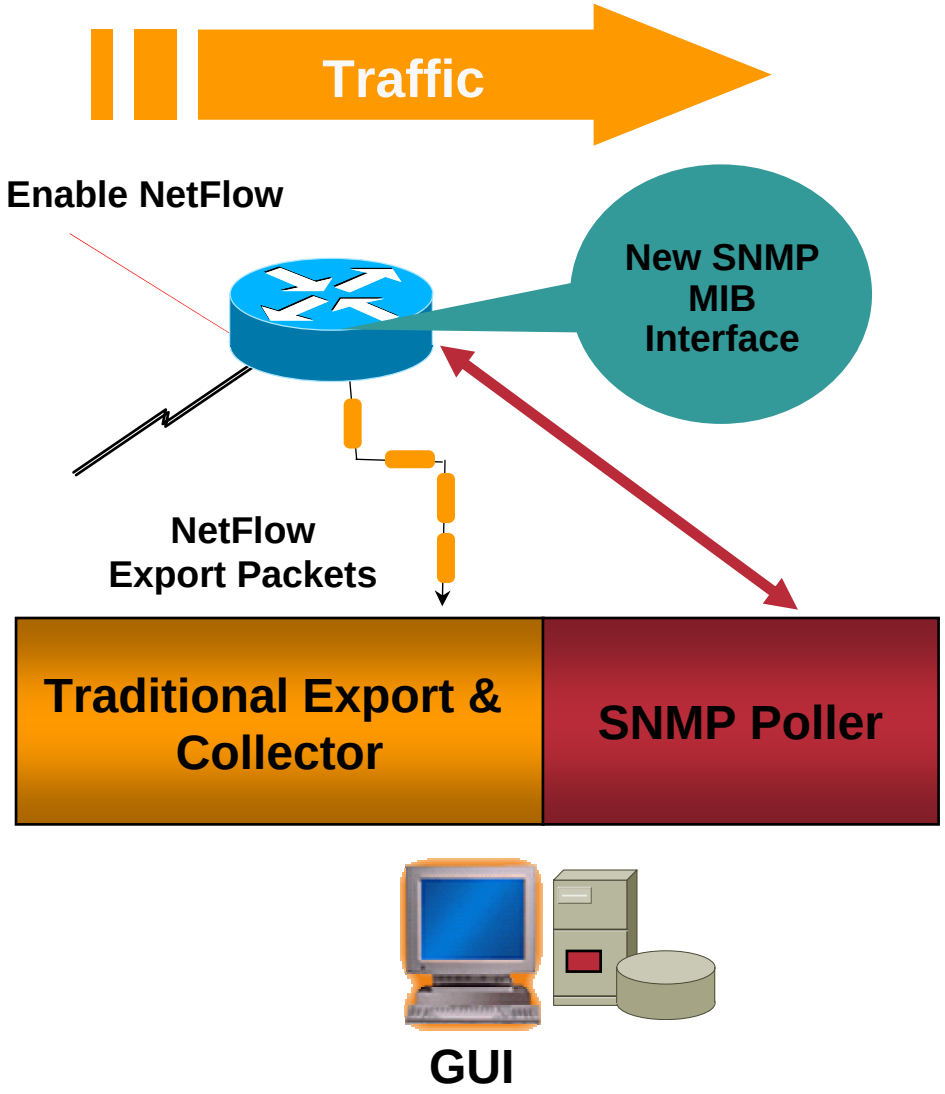
Key Concept - NetFlow Scalability

Cisco.com

- 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

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A 2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A 1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

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

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Aggregation

No

Yes

e.g. Protocol-Port Aggregation Scheme Becomes

Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	00A2	1528

Aggregated Flows—Export Version 8 or 9

4. Export version

Non-Aggregated Flows—Export Version 5 or 9

5. Transport protocol

Export Packet

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

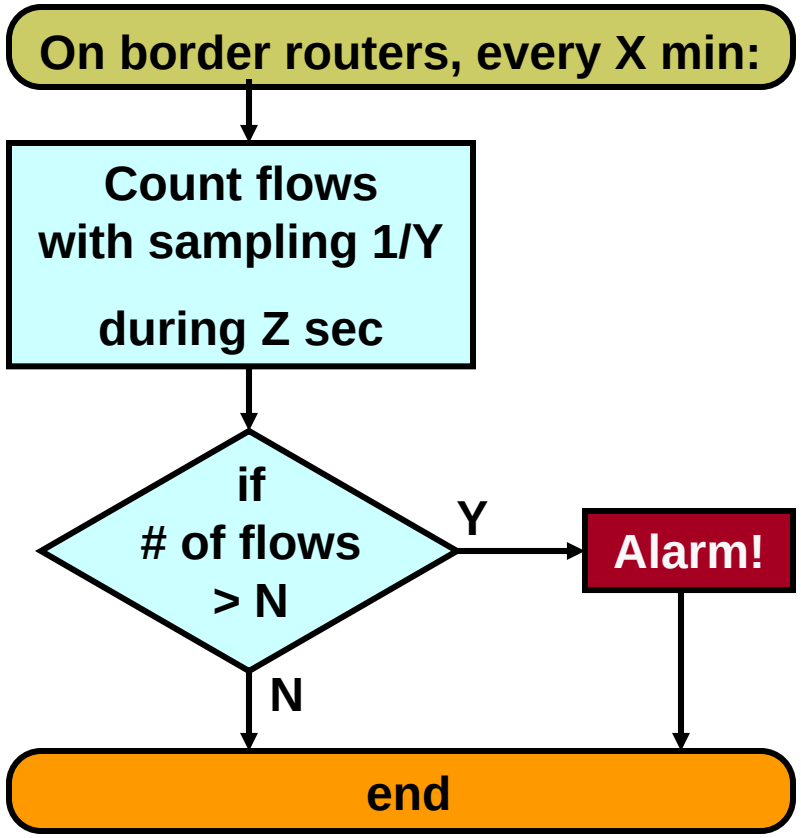
NetFlow is Useful for Security

Cisco.com

- 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



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: …

Real data deleted in this presentation

src_ip	dst_ip	in int	out int	src port	dest port	pkts	bytes	prot	src_as	dst_as
192.xx.xxx.69	194.yyy.yyy.2	29	49	1308	77	1	40	6	xxx	ddd
192.xx.xxx.222	194.yyy.yyy.2	29	49	1774	1243	1	40	6	xxx	ddd
192.xx.xxx.108	194.yyy.yyy.2	29	49	1869	1076	1	40	6	xxx	ddd
192.xx.xxx.159	194.yyy.yyy.2	29	49	1050	903	1	40	6	xxx	ddd
192.xx.xxx.54	194.yyy.yyy.2	29	49	2018	730	1	40	6	xxx	ddd
192.xx.xxx.136	194.yyy.yyy.2	29	49	1821	559	1	40	6	xxx	ddd
192.xx.xxx.216	194.yyy.yyy.2	29	49	1516	383	1	40	6	xxx	ddd
192.xx.xxx.111	194.yyy.yyy.2	29	49	1894	45	1	40	6	xxx	ddd
192.xx.xxx.29	194.yyy.yyy.2	29	49	1600	1209	1	40	6	xxx	ddd
192.xx.xxx.24	194.yyy.yyy.2	29	49	1120	1034	1	40	6	xxx	ddd
192.xx.xxx.39	194.yyy.yyy.2	29	49	1459	868	1	40	6	xxx	ddd
192.xx.xxx.249	194.yyy.yyy.2	29	49	1967	692	1	40	6	xxx	ddd
192.xx.xxx.57	194.yyy.yyy.2	29	49	1044	521	1	40	6	xxx	ddd
…	…	…	…	…	…	…	…	…	…	…

Tracing Back with Netflow

- **Routers need Netflow to be enabled**

Victim

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

The flows come from serial 1

Find the upstream router on 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
```

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 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-X                2      0.0         1  1440      0.0       0.0       9.5
TC                82580     11.2         1  1440     11.2       0.0      12.0
To                82582                           11.2       0.0      12.0

Sr  SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et  132.122.25.60   Se0/0         192.168.1.1     06 9AEE 0007     1
Et  139.57.220.28   Se0/0         192.168.1.1     06 708D 0007     1
Et  165.172.153.65  Se0/0         192.168.1.1     06 CB46 0007     1
```

Source Interface

Flow info summary

Flow details

SrcIf
Et0/0
Et0/0
Et0/0

show ip cache verbose flow


```
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 1.00 .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
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-other        22210      3.1         1  1440      3.1       0.0      12.9
Total:           22210      3.1         1  1440      3.1       0.0      12.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr TOS Flgs  Pkts
Et0/0         216.120.112.114 Se0/0         192.168.1.1     06 00  10      1
5FA7 /0  0                    0007 /0  0    0.0.0.0               1440     0.0
Et0/0         175.182.253.65  Se0/0         192.168.1.1     06 00  10      1
```

Port Msk AS Port Msk AS NextHop B/Pk Active

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.com

- 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

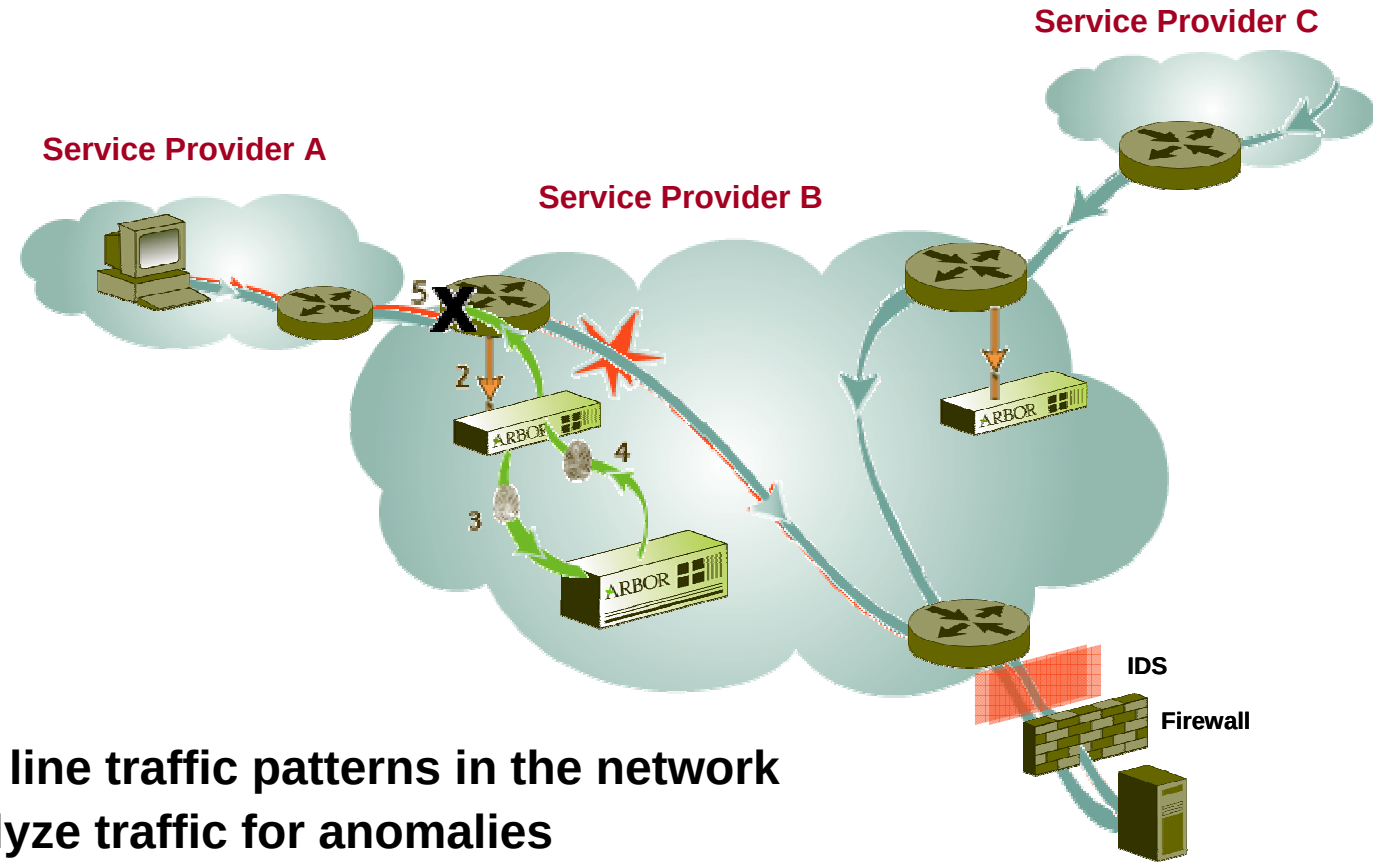
  DoS attacks flood the network with packets, often of an unusual size, from an untrusted source to a single destination
- Cisco detects and prevents DoS attacks by using Cisco IOS NetFlow to collect:

  Packet source Port number

  Destination Packet size

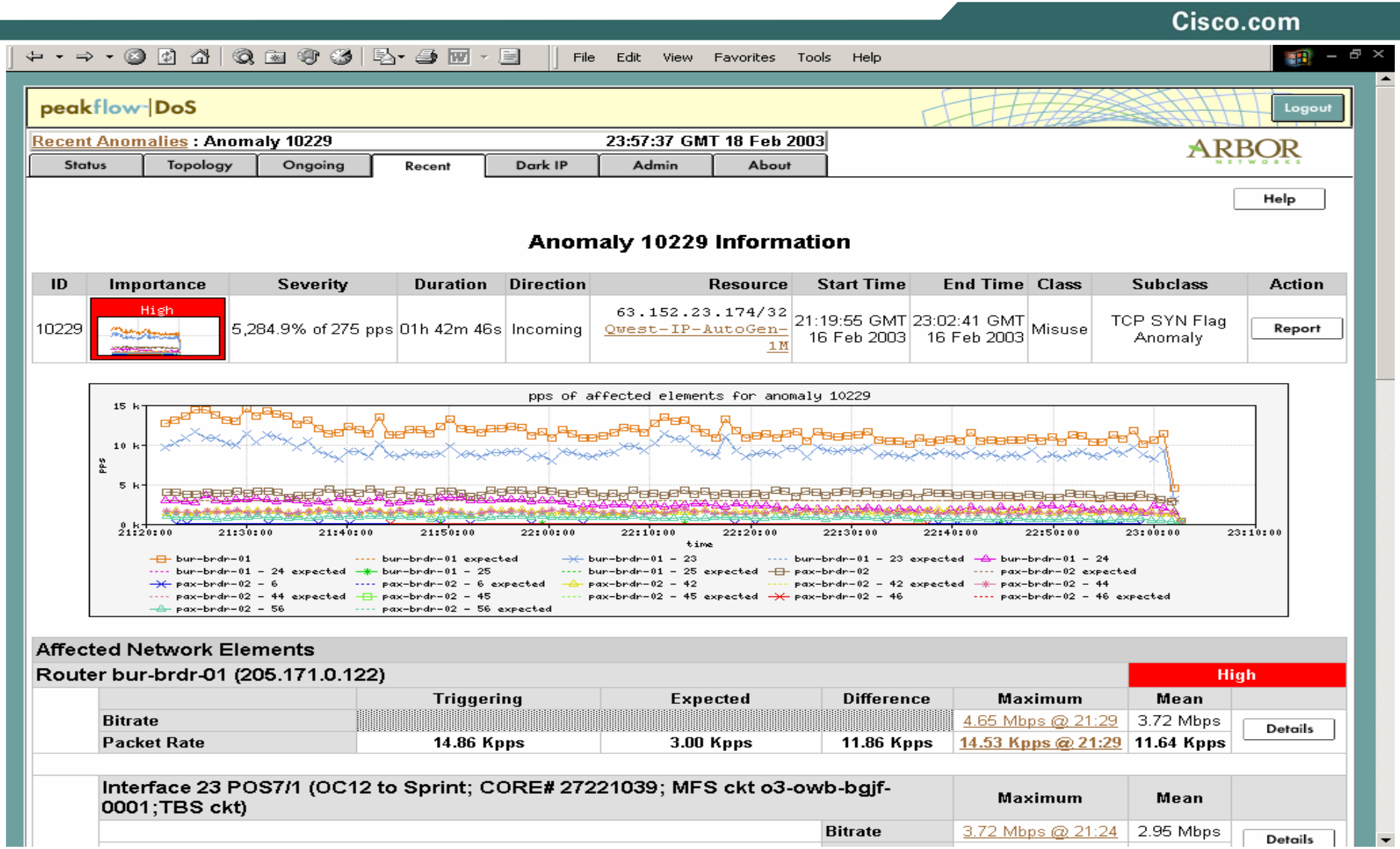
  Protocol number
- Collected information is sent to Arbor Peakflow DoS for anomaly detection

Arbor Networks: Service Provider Solution



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



Protego Networks Tracing Attack

Incident Graph-245738986

Previous | Next | Toggle Topology

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:

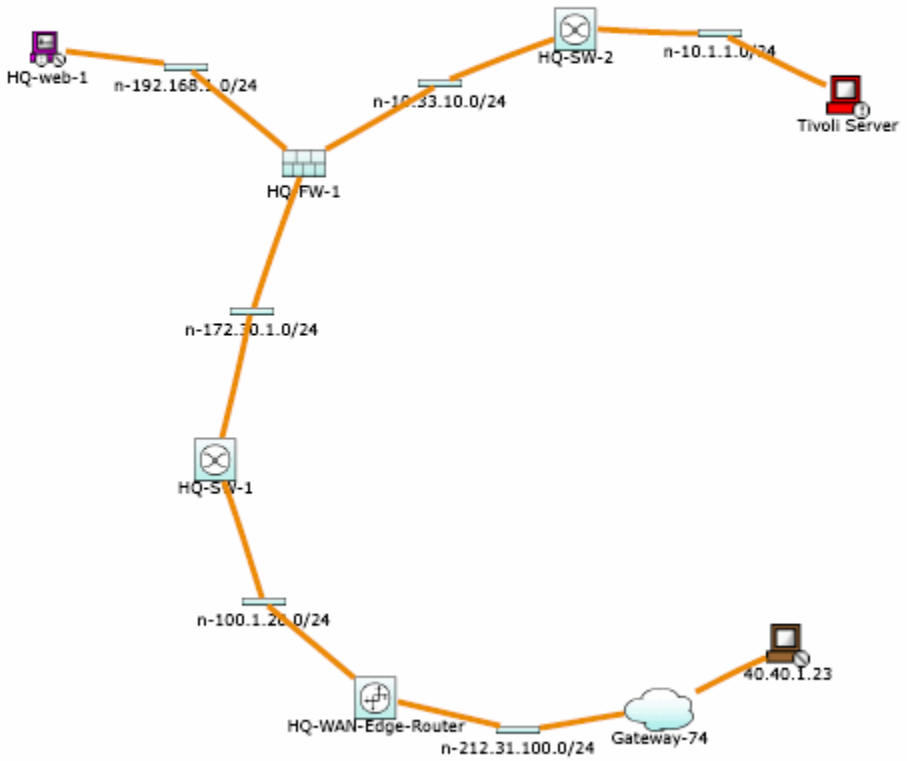
ICMP Ping Network Sweep

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



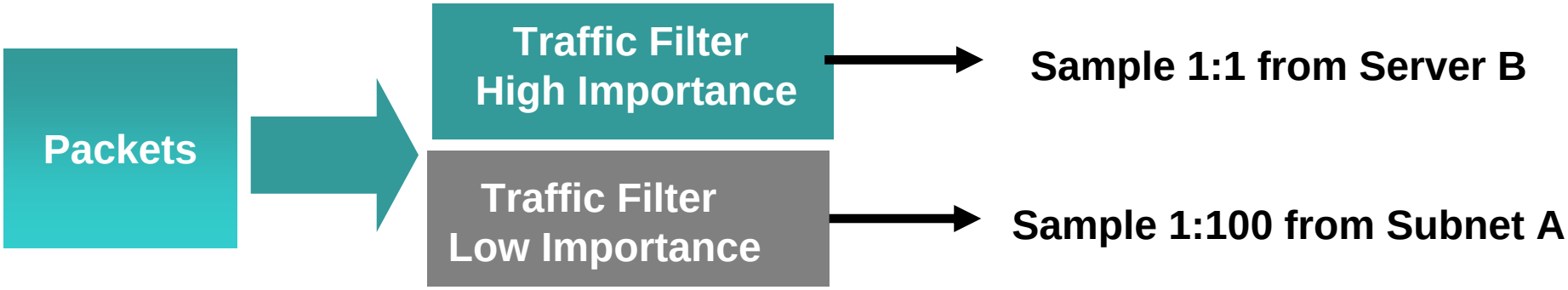
www.protegonetworks.com

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



References

- www.cisco.com/go/netflow