IP Flow Monitoring
Objectives

Participants will understand:

• Why we monitor & analyse IP flows
• Tuples, netflow versions, & IPFIX
• How flow monitoring works
• Flow alerting & analysis
• Popular tools for flow monitoring
What's an IP Flow?

A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device.

-- B. Clase, RFC3954

A Flow is defined as a set of packets or frames passing an Observation Point in the network during a certain time interval. All packets belonging to a particular Flow have a set of common properties.

-- B. Clase, B. Trammel, P. Aitken, RFC7011
Why do we Monitor IP Flows?

• Where is our traffic coming from?
  – Google? Facebook? (Are we well-connected to them?)

• What kind of application traffic is it?
  – Mail? HTTPS? VoIP?

• Are the correct QoS bits set?

• Have routing changes impacted the network?
Why do we Monitor IP Flows?

• Are some hosts abusing our network?
• Are they running insecure protocols?
• Do they have far more flows than they should?
• Are they participating in a DDoS?
To find what our traffic is
To find hosts participating in DDoS
To find traffic’s Geographic Origin
To find traffic’s ASN Origin
Know a Flow by its Tuple

- Source IP Address
- Destination IP Address
- Protocol
- Source Port
- Destination Port
- Class or Type of Service
- Router or switch ingress interface
Know a Flow by its Tuple

| Ethernet II, Src: b8 69:4f:1e:7c:6f (b8:69:4f:1e:7c:6f), Dst: Cisco_f0:e4:00 (00:12:7f:00:e4:00) |
| Internet Protocol Version 4, Src: 190.27.27.225 (205.27.27.225), Dst: 64.233.186.189 (64.233.186.189) |
| Version: 4 |
| Header Length: 20 bytes |
| Differentiated Services Field: 0x00 (Default: ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) |
| Total Length: 57 |
| Identification: 8x57f2 (22514) |
| Flags: 0x00 |
| Fragment offset: 0 |
| Time to live: 63 |
| Protocol: UDP (17) |
| Header checksum: 0x441f [validation disabled] |
| Source: 290.27.27.225 (200.27.27.225) |
| Destination: 64.233.186.189 (64.233.186.189) |
| [Source GeoIP: Unknown] |
| [Destination GeoIP: Unknown] |
| User Datagram Protocol, Src Port: 55085 (55085), Dst Port: 443 (443) |
| Source Port: 55085 (55085) |
| Destination Port: 443 (443) |
| Length: 37 |
| Checksum: 0x7a7a [validation disabled] |
| [Stream index: 0] |
| QUIC (Quick UDP Internet Connections) |
What’s Netflow?

• Cisco protocol for flow monitoring released in 1996
• Described by RFC 3954, but not an Internet Standard
• Netflow V5 is supported by nearly all router platforms
• Versions in use include:
  – Version 5: IPv4 Only
  – Version 9: IPv4/v6 & MPLS
What’s IPFIX?

• IP Flow Information Export
• Vendor neutral protocol for flow monitoring
• Started through the IETF process in 2004 & released in 2011
• Based on Cisco's Netflow Version 9
• IPFIX is an Internet Standard replacement for Netflow 9
How do NetFlow & IPFIX Work?

- Packets with matching tuples are grouped into a flow
- First occurrence of a flow is recorded in a flow cache
- Cache entries are timestamped
- Number of packets & bytes matching the flow are tallied
- Details like next hop IP, ASN, subnet masks, TCP flags can be recorded
- Cache can be queried interactively, or flows can be exported
Setting Up Netflow & IPFIX

- Alcatel Cflowd Configuration Overview
- Cisco Netflow Configuration Guide
- Dell Force 10 sFlow Setup
- Dell EMC N Series sFlow Setup
- Huawei Netstream Configuration
- Juniper Monitoring, Sampling, and Collection Services Feature Guide
- Linux Softflowd Setup
- Mikrotik IP Traffic Flow
Flow Sampling / Downsampling

• Tracking every flow can take a lot of device resources
• Some routers & switches can be crippled by turning on Netflow
• Sampling helps by tracking one in n packets, where n = 1-65535
• CPU load can be significantly reduced - but so can resolution.
Softflowd: Software Flow Monitoring

- **Softflowd** is a passive Netflow collector
- Not all devices support Netflow directly
- Network traffic passing through a switch can be mirrored
- Attach a Unix computer to the mirrored port
- Softflowd tracks flows from the mirrored traffic
- Flows can be exported just as they are from routers & switches
Ad-Hoc Flow Queries

• Some platforms allow you to directly query flow stats
  – Cisco `show ip flow`
  – Junos `show services accounting flow-detail`

• Where that's not possible, free & low-cost tools exist:
  – FlowStats for MacOS (only supports v5)
Long-Term Flow Analysis

- **nfdump**: FOSS application to collect and process netflow & sflow
  - C application that receives flows & logs them to files
- **nfsen**: FOSS application to generate stats & display graphs
  - Web application written in Perl & PHP, depends on nfdump
- **ntopng**: FOSS + Commercial Flow Collector & Traffic Analyser
  - Monitor & generate alerts on flow thresholds
  - Netflow collector requires a license
- **flowanalyzer**
- Elastiflow
- Rock NSM
nfdump + nfsen
Additional Resources

• Introduction to Cisco IOS NetFlow: A Technical Overview

• Fundamentals of Netflow: eTutorial

• SANS For572: network forensics with Netflow on ELK stack