

Flow based Traffic Analysis

Muraleedharan N
C-DAC Bangalore
Electronics City
murali@ncb.ernet.in

Challenges in Packet level traffic Analysis

- Network traffic grows in volume and complexity
- Capture and decode every packets for traffic analysis is one of the challenge in a high speed network
- In analysis point of view, the volume of data for analysis if huge.
- This will have an impact on performance of the analysis.

Introduction To Flow Based Traffic Analysis

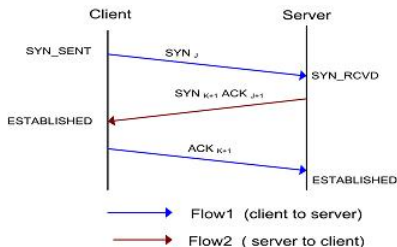
Definition

flow is a unidirectional series of IP packets of a given protocol travelling between a source and a destination IP/port pair within a certain period of time.

- Aggregate information from different packets in to a flow
- Different levels of analysis can be possible
- Compared to packet based analysis , volume of data is very less
 - Suitable for high speed traffic analysis

Introduction

- Since flow is unidirectional every TCP connection will create at least two flows.



- Source to Destination
- Destination to Source

Flow Parameters

Flow Parameters

IP Header

4-bit	8-bit	16-bit	32-bit	
Ver.	Header Length	Type of Service	Total Length	
Identification		Flags	Offset	
Time To Live	Protocol	Checksum		
Source Address				
Destination Address				
Options and Padding				

TCP Header

Source Port		Destination Port						
Sequence Number								
Acknowledgement Number (ACK)								
Offset Reserved	U	A	P	R	S	F	Window	

UDP Header

0	Source Port	Destination Port
32	Length	Checksum

Flow Record

Source Address		
Destination Address		
Source Port		Destination Port
Protocol	TOS	Other Aggregated Values

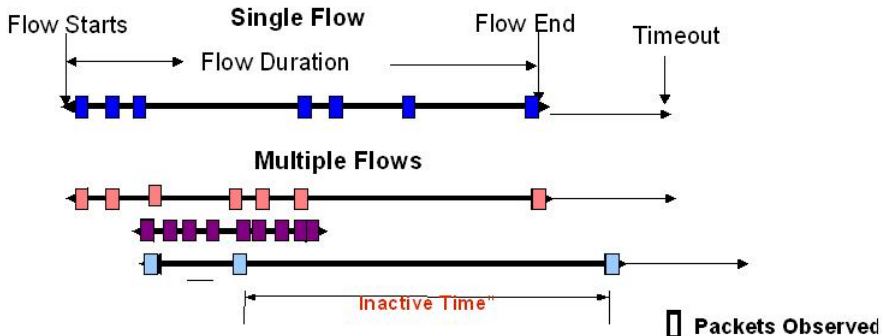
Flow can be defined using following parameters

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Protocol

Other than these parameters flow contains

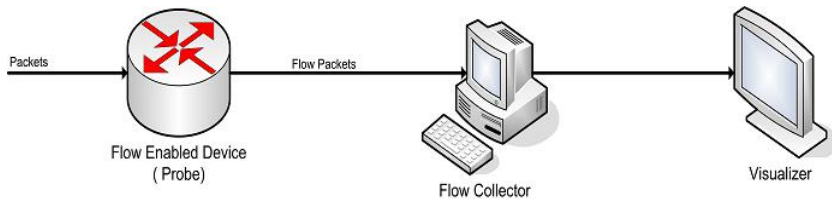
- Start and end time
- Duration
- Number of packet transferred
- Number of Bytes transferred
- TCP Flag Values

Flow Components



Date	Time	Duration	Protocol	Src IP	Dst IP	Src Port	Dst Port	Pkt	Bytes	TCP Flags
2008-09-10	15:25:35.466	24.123	TCP	72.14.207.127	172.16.1.9	80	51282	7	12800	.AP.SF
2008-09-10	15:25:20.916	24.963	UDP	172.16.1.4	212.234.91.123	1024	53	9	593
2008-09-10	15:25:23.527	11.123	ICMP	202.141.151.30	172.16.1.4	0	8.0	2	12800

Flow Components

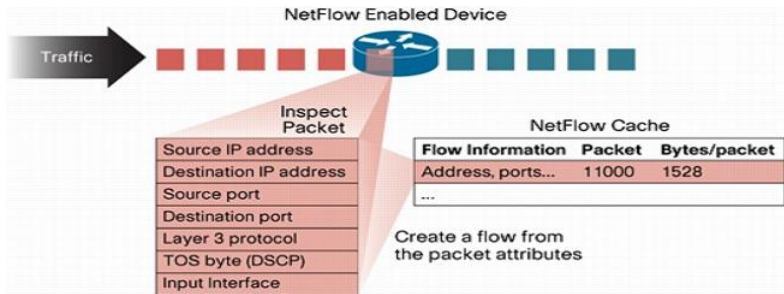


Flow Components

- Flow Probe
 - Collects and decode packets from the network
 - Aggregate packets in to flow using flow key
 - Export flow data into flow collector
- Flow Collector
 - Collects and decode flow packets
 - Store Flow records for further analysis
 - Provides data in to flow analyzer
- Flow Analyzer
 - Doing analysis on flow records
 - Performance
 - Security
 - QoS
 - Visualize the Analysis Output

- Different vendor specific flow definitions and exporting mechanisms are available
 - Netflow from Cisco
 - Sflow from Inmon
 - Jflow from Juniper

- NetFlow is one of the most widely used flow measurement solution defined by cisco

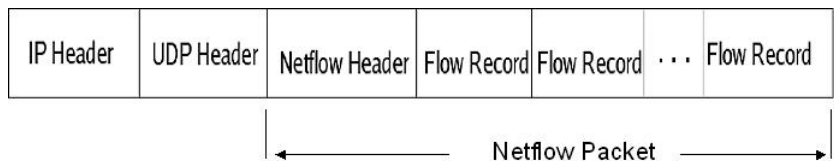


Netflow Versions

No	Version	PropertiesS
1	Version1	
2	Version5	Commonly used
3	Version6	Encapsulation Information
4	Version7	Switch information
5	Version8	Many Aggregation functions
6	Version9	Template Based , Defined in RFC 3954

- Selects **sampled packets** for creating flows
- Using this method devices does not have to cache all flows.
- Mainly used for monitoring purpose.
- Can provide layer 2 parameters
- Based on the structure of probe and collector
- The probe only sends a sampled packet to the collector.

Flow Exporting methods



- Commonly uses UDP packet for exporting flow records
- Multiple flow record can be embedded in a single UDP packets

Flow Exporting methods

- The flow information collected from the device (switch/Router) has to send to the flow collector.
- **IPFIX** is a protocols which defines how IP flow information can be exported from routers, measurement probe or other devices

IPFIX IP Flow Information Export

- Provides a common standard for exporting flow
- Specified by IPFIX working group
- Supporting Cisco NetFlow version 9
- IP Flow Information Export (IPFIX) Implementation Guidelines Defined in **RFC 5153**
- Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information defined in **RFC 5101**

- Supports user defined parameters
- Supports template based header
- Becoming a standard exporting protocol
- Application is not limited to flow

- Behaviour Analysis
 - Network Behaviour
 - Application Behaviour
 - Host behaviour
- Performance Analysis
- Security Analysis

Network Behaviour analysis

- What is the normal traffic pattern in the network
- At what time the network traffic is maximum / minimum
- How many machines are active in the network for a particular time
- Average connection duration
- Protocol and application distribution
- Flow Parameters date, time , duration,protocol, no of bytes, no of packets, No of flows

Performance Behaviour analysis

- Bandwidth usage for a particular time
- Incoming and Outgoing traffic
- Maximum /Average Link utilization
- Packet rate
- Number of connection request
- Who is generating and receiving more traffic

Application Behaviour analysis

- Behaviour of applications are different
 - File transfer
 - Web Application
 - P2P Application
- Identify what is the application distribution of the network traffic
- Flow Parameters
 - Port numbers, protocol, no of bytes, no of packets

Host Behaviour analysis

- How many incoming connection to a host for a particular time duration
- Number of outgoing connection from a host
- Commonly using application and protocols
- Flow Parameters
 - Source and Destination IP
 - Source and Destination port
 - Flow Duration,
 - Protocol
 - No of Flows

- Scan Detection
- DoS / DDoS Detection
- Spreading of Malwares
- Botnet Detection
- Baseline Traffic
- Application Usage
- Port level auditing
- Inappropriate Usage
 - Free Data Hosting
 - Remote Desktop Access

- Traffic analysis can be used to detect network traffic anomaly.
- Identify the normal traffic patterns in a network
- Any deviation from the normal traffic pattern can be considered as an anomaly
- Changes in the normal network pattern can be occur due to different attacks.
- These types of attacks cannot be detect using signature based detection techniques

Different types of attacks identified by anomaly detection:

- Scan
 - Network scanning is a procedure for identifying active hosts and services on a network or host.
- Flow Parameters.
 - Number of flows
 - Packet Size
 - Duration
 - Source and Destination Port
 - Source and Destination IP

Flooding Attacks

- In a flooding attack, the attacker sends large amounts of bogus traffic toward the victims network to consume its bandwidth, exploiting the lack of bandwidth resource management in IP networks.
- Denial of Service Attacks (DoS)
- Distributed Denial of Service (DDoS)
- Flow Parameters.
 - Number of flows
 - Source and Destination Port
 - Duration
 - Packet length
 - Source and Destination IP

- Flow Probe
 - fprobe
 - Open source tool for flow creation
- Flow Collector
 - nfdump toolkit
 - nfcapd - Netflow capture daemon netflow packet collector
 - nfdump - Providing text data of flow records
- SiLk (System for Internet Level Knowledge) tool kit
 - Developed by CERT Network Situational Awareness Team
 - YAF (Yet Another Flow meter)

- libfixbuf
 - From CERT
 - C Libraries are available
- libipfix
 - Implementation of IPFIX
 - C and Java Libraries are available

Conference
floConf by CERT



RFC 5101 - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information .



RFC3954 - Cisco Systems NetFlow Services Export Version 9



*Traffic Monitoring using sflow -
www.sflow.org/sFlowOverview.pdf*



*Introduction to Cisco IOS NetFlow - A Technical Overview -
<http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps65>*



A parameterizable methodology fo Internet traffic flow profiling - KC Claffy, HW Braun, GC Polyzos,- Selected Areas in Communications, IEEE Journal - OCTOBER 1995