Contents

NetFlow

Definition

A network flow is defined as a unidirectional sequence of packets between given source and destination endpoints. Network flows are highly granular. Traditional NetFlow uses a 7-tuple of source and destination IP address, transport layer port numbers, IP Protocol, Type of Service (ToS), and the input interface port to uniquely identify flows. (Egress NetFlow uses the output interface.)

Flexible NetFlow (FNF) is a ground-up rewrite of NetFlow which allows the user to customise the netflow tuple to include (or exclude) almost 200 different fields.

NetFlow data can be exported to a NetFlow Collector appliance in a variety of cisco defined formats (v1, v5, v8, v9 (RFC 3954)), or in the standardised IPFIX format (RFC 5101). Data is most often transferred over UDP or SCTP-PR (RFC3758).

NetFlow Switching

Conventional network layer switching handles incoming packets independently, with separate serial tasks for switching, security, services, and traffic measurements applied to each packet. With NetFlow switching, this process is applied only to the first packet of a flow. Information from the first packet is used to build an entry in the NetFlow cache. Subsequent packets in the flow are handled via a single streamlined task that handles switching, services, and data collection concurrently. However, NetFlow switching has largely been superceded by fast and CEF switching.

Purpose

Today, NetFlow (and now, FNF) are largely used for accounting, auditing, monitoring and security.

Sites

- Cisco NetFlow page
- Cisco Flexible NetFlow page
- NetFlow RFC
- IP Flow Information Export (IPFIX) Protocol (IPFIX) RFC

- Stream Control Transmission Protocol (SCTP) Partial Reliability Extension RFC

Related Resource

Cisco Trademarks