What are NetFlow and sFlow Protocols?

NetFlow and sFlow are both network monitoring technologies that provide insights into network traffic and performance.

NetFlow, developed by Cisco, is a protocol that collects and analyzes network traffic data, allowing organizations to understand traffic patterns, detect anomalies, and optimize network performance.

On the other hand, sFlow is a more open and vendor-neutral protocol for monitoring network traffic. It samples packets at the interface level and provides a broader view of network activity, including detailed information on the types of traffic and the devices generating it.

Benefits of NetFlow and sFlow

Network monitoring and traffic analysis offer insights into traffic, and help you understand network behavior.

Monitoring Network Applications and Use

The data collected through NetFlow or sFlow enables you to view comprehensive, time- and application-based insights into network usage. This data serves as a foundation for strategic network and application resource allocation, offering robust near real-time monitoring capabilities. It can effectively display traffic trends and views based on applications. Additionally, it facilitates proactive identification of issues, streamlined troubleshooting, and swift problem resolution. This information proves invaluable in optimally allocating network resources, as well as identifying and addressing potential security breaches and policy violations.

Network Planning

NetFlow or sFlow can be effectively used to capture data over extended durations, empowering users to monitor and predict network expansion, and plan enhancements such as increased routing devices, ports, or higher-bandwidth interfaces. The data serves as a cornerstone for fine-tuning network planning, including aspectssuch as peering, backbone upgrades, and routing policy decisions. This approach minimizes overall network operational costs while maximizing performance, capacity, and reliability. The data aids in identifying unwanted WAN traffic, validating bandwidth and Quality of Service (QoS), and facilitating analysis of novel network applications. This wealth of information ultimately contributes to reducing the network operation costs.

Security Analysis

NetFlow or sFlow data plays a pivotal role in promptly detecting and categorizing real-time Denial of Service (DoS) attacks, viruses, and worms. Changes in network patterns reveal anomalies that are distinctly highlighted in the NetFlow data. Furthermore, this data is an invaluable resource for network forensic analysis, enabling a comprehensive understanding and reconstruction of security incidents.

Billing and Accounting

Provides insights into the utilization of resources across a network, and facilitating detailed accounting reports depicting resource usage across diverse network components.

Traffic Engineering

NetFlow and sFlow can gauge the volume of traffic traversing peering or transit points, and assess whether a peering agreement with other service providers is fair and equitable.

Key Components of NetFlow and sFlow

The following NetFlow and sFlow components help you capture, export, collect, analyze, and manage data:

Flow Exporter

The flow exporter, also referred to as an exporter map, functions as a device tasked with collecting data regarding network flows. It transfers the compiled flow records to the designated collector. The exporter is responsibile for inspecting packets, identifying flows, and exporting flow-related data. The exporter map can transmit flow reports to a single destination. A maximum of 8 exporters are permitted per MAP configuration.

Contained within a flow exporter are particulars outlining network specifications and transport layer attributes related to the packets. These packets are exported to the collector through the utilization of the User Datagram Protocol (UDP) transport protocol. In cases where the source interface does not have an assigned IP address, the packet exporter remains inactive.

Flow Monitor

A flow monitor, also referred to as a Monitor map, serves the purpose of facilitating active traffic monitoring on a pre-configured interface. After the flow monitor is commited to an interface, a corresponding flow monitor cache is generated. This cache is used to collect traffic data based on both key and non-key fields outlined within the configured record.

A monitor map contains name references that link to the flow record map and flow exporter map, both of which are committed to an interface. If an exporter map is not applied to the monitor map, the flow records are not exported. In such cases, the aging process adheres to the cache parameters specified in the monitor map.

Furthermore, the option to include extended details such as router-specific elements like nexthop, source and destination mask lengths, and extended gateways attributes, including nexthop, communities, local preference, and AS (source AS, source peer AS, and destination AS path) information.

Flow Sampler

The sampler map specifies the rate at which packets (one out of n packets) are sampled. The sampler map configuration is typically geared for high-speed interfaces to optimize CPU utilization. To achieve this, start by setting the sampling rate after evaluating your network parameters such as traffic rate, number of total flows, cache size, active and inactive timers.

- The maximum supported sampling rate is 1:1, where every packet is processed.
- The minimum supported sampling rate is 1:262,144, indicating that only one out of every 262,144 packets is processed.

Consider these points before applying the sampler map:

- Remove any existing Netflow or sFlow configurations before applying a new sampler map on an interface.
- Use the same sampler map configuration on the sub-interfaces and physical interfaces under a port.