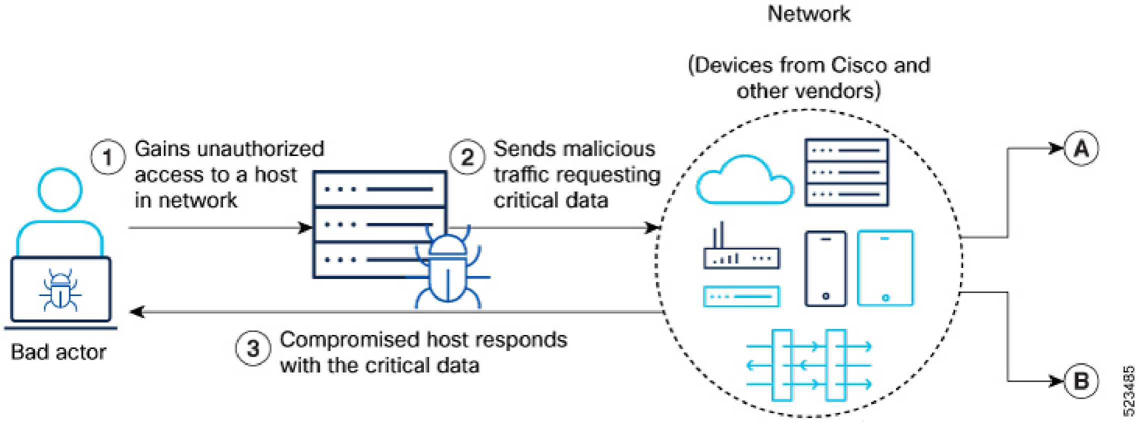
Use Case: NetFlow and sFlow in Action

Here's a hypothetical use case illustrating a bad actor (attacker) sending malicious traffic and the network getting compromised:

Figure 1: Malicious activity in a network


Network
(Devices from Cisco and other vendors)
1 Gains unauthorized access to a host in network
2 Sends malicious traffic requesting critical data
3 Compromised host responds with the critical data
Bad actor
A
B
523485

1 Scenario A: Traffic Monitoring Without NetFlow and sFlow

2 Scenario B: Traffic Monitoring With NetFlow and sFlow

- Attack entry point—An Enterprise becomes the target of a cyber attack. The attacker employs various tactics to gain unauthorized initial access to the network.
- Generate malicious traffic— After the attacker identifies vulnerable devices as potential targets, they compromise a host and start generating malicious traffic and potentially launch DDoS attacks, to steal sensitive data, or take control of the network using these compromised machines as a platform.
- Breach data—The malicious traffic triggers a series of attacks within the network. With access to sensitive data, the attacker attempts retrieving critical data from the compromised network.

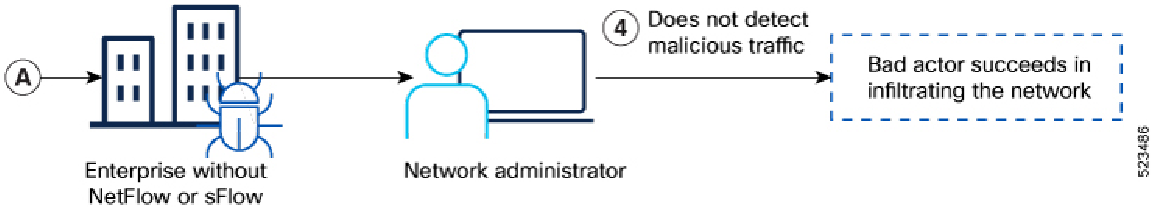
With this context, lets explore these two scenarios:

- Scenario A: Traffic Monitoring Without NetFlow and sFlow, on page 2
- Scenario B: Traffic Monitoring With NetFlow and sFlow, on page 2

Scenario A: Traffic Monitoring Without NetFlow and sFlow

In this particular situation, the enterprise had failed to implement any network traffic monitoring protocols such as NetFlow or sFlow.

Figure 2: Traffic monitoring without Flow data to identify malicious activity


A
Enterprise without NetFlow or sFlow
Network administrator
4
Does not detect malicious traffic
Bad actor succeeds in infiltrating the network
523486

Here is a high-level outline of the network's response to the attack:

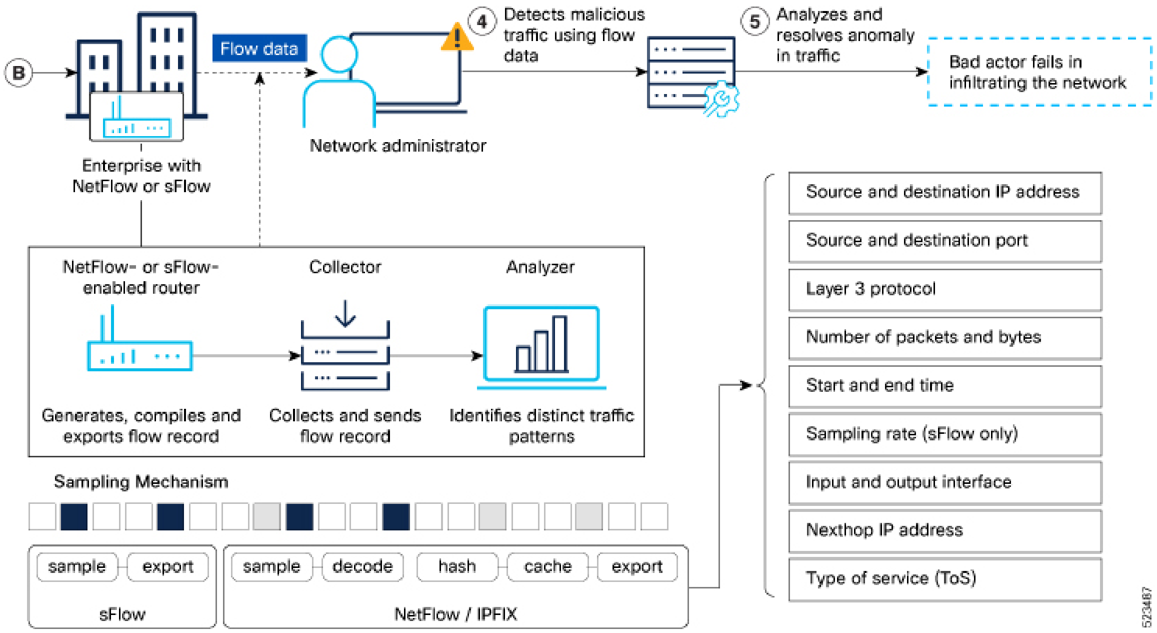
- Bypassed threat detection and response—The network administrator does not detect any unusual network patterns or intrusions immediately following the attack.
- Successful data breach—Consequently, the network is compromised through malicious traffic that gets undetected leading to loss of critical data and trust.

The overall network security posture is compromised due to lack of traffic monitoring mechanisms leading to poor visibility of the network and its functionalities.

Scenario B: Traffic Monitoring With NetFlow and sFlow

In this particular situation, the enterprise has implemented network traffic monitoring protocols such as NetFlow or sFlow.

Figure 3: Traffic monitoring workflow with Flow data to identify malicious activity


B
Flow data
Enterprise with NetFlow or sFlow
Network administrator
4 Detects malicious traffic using flow data
5 Analyzes and resolves anomaly in traffic
Bad actor fails in infiltrating the network
NetFlow- or sFlow-enabled router
Collector
Analyzer
Generates, compiles and exports flow record
Collects and sends flow record
Identifies distinct traffic patterns
Sampling Mechanism
sample
export
sFlow
sample
decode
hash
cache
export
NetFlow / IPFIX
Source and destination IP address
Source and destination port
Layer 3 protocol
Number of packets and bytes
Start and end time
Sampling rate (sFlow only)
Input and output interface
Nexthop IP address
Type of service (ToS)
523487

Here is a high-level outline of the network's response to the attack:

- Flow data collection—Routers enabled with NetFlow or sFlow capture and retain flow records of transmitted traffic. These records store essential metadata related to the traffic's journey, including source and destination domains, the count and volume of inbound and outbound packets, timestamps and so on. The recorded flow records are then sent to a designated collector.
- Data analysis—Utilize a NetFlow or sFlow analyzer or security monitoring tool to process and analyze the collected data. The tool can identify patterns and anomalies that may indicate a security threat, such as unusual traffic patterns, unexpected communication between hosts, or a high volume of traffic from suspicious sources.
- Threat detection—The analyzer applies algorithms and rules to detect potential threats based on the analyzed data. It can compare network traffic with predefined security policies. If a potential threat is detected, the analyzer generates an alert. This alert can be sent to the network administrator for further investigation.
- Prompt investigation and responsive action—Upon receiving the alert, the network administrator can investigate the identified threat. They can analyze additional logs, inspect packet captures, or perform other security measures to gather more information about the threat. Once the threat is confirmed, appropriate actions can be taken to mitigate the impact by blocking the malicious IP addresses and isolating affected hosts to prevent further harm.

By leveraging NetFlow and sFlow for threat identification, you can proactively detect and respond to security threats, enhancing the overall network security posture. It allows for early threat detection, and faster incident response, ultimately reducing the risk of a successful attack.