JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Introduction To NetFlow For CyberSecurity

**Prathamesh Anant Palvankar**
Department Of IT
GMVCS

**Pranit Naresh Kadam**
Department Of IT
GMVCS

**Shraddha Ravindra Palkar**
Department Of IT
GMVCS

**Madiha Murad Maner**
Department Of IT
GMVCS

**Ketaki Genaji Nadkar**
Department Of IT
GMVCS

## Abstract

NetFlow, originally developed by Cisco, is a network protocol for collecting IP traffic information and monitoring network flow. Its application in cybersecurity has grown significantly, providing essential insights for detecting and mitigating various network threats. This abstract delves into the utility of NetFlow data in enhancing cybersecurity measures by offering comprehensive network visibility, anomaly detection, and incident response capabilities. NetFlow captures detailed information about network traffic, including source and destination IP addresses, ports, and protocols. This visibility is crucial for identifying normal versus abnormal traffic patterns, facilitating a robust understanding of network behaviour. NetFlow data aids in the swift investigation of security incidents. By providing historical traffic records, security teams can trace the origin and impact of attacks, enhancing their ability to respond effectively and mitigate damage. NetFlow integrates seamlessly with other security solutions like intrusion detection systems (IDS), security information and event management (SIEM) systems, and threat intelligence platforms. This integration amplifies the capability to correlate network events with security alerts, providing a more comprehensive defence strategy. NetFlow's lightweight data collection methodology allows it to scale across large networks without significantly impacting performance. This scalability ensures that even expansive network environments can benefit from its detailed traffic analysis capabilities.

**Keyword –** NetFlow, Cybersecurity, Network Traffic Analysis, Network Visibility, Incident Response, Network Security.

## 1. Introduction

NetFlow is a Cisco technology that provides comprehensive visibility into all network traffic that traverses a Cisco-supported device. Cisco invented NetFlow and is the leader in IP traffic flow technology. NetFlow was initially created for billing and accounting of network traffic and to measure other IP traffic characteristics such as bandwidth utilization and application performance. NetFlow has also been used as a network-capacity planning tool and to monitor network availability. NetFlow is used by many cybersecurity professionals as a network security tool because its reporting capabilities provide nonrepudiation, anomaly detection, and investigative capabilities. As network traffic traverses a NetFlow-enabled device, the device collects traffic flow information and provides a network administrator or security professional with detailed information about such flows.

**NetFlow provides detailed network telemetry that allows the administrator to do the following:**

- See what is actually happening across the entire network.
- Identify DoS attacks.
- Quickly identify compromised endpoints and network infrastructure devices.
- Monitor network usage of employees, contractors, or partners.

- Obtain network telemetry during security incident response and forensics.
- Detect firewall misconfigurations and inappropriate access to corporate resources.

**NetFlow supports both IP version 4 (IPv4) and IP version 6 (IPv6), and it plays a crucial role in the following:**

- Network planning
- Network security
- Network troubleshooting
- Traffic engineering

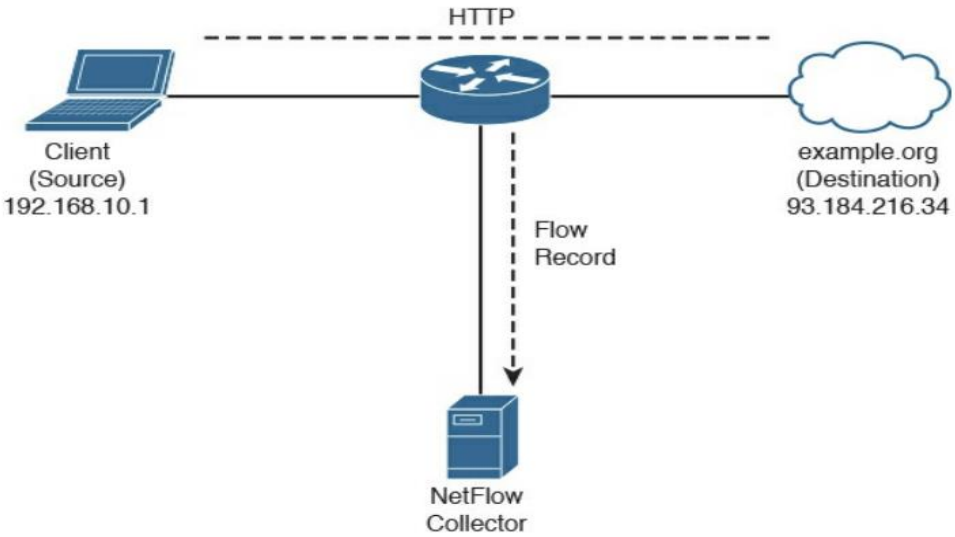
## 1. Literature Review

NetFlow, developed by Cisco, is a network protocol designed for the collection and monitoring of IP traffic. Its relevance in the field of cybersecurity has grown as organizations seek more sophisticated methods to detect and mitigate network-based threats. This literature review examines the current state of research on the application of NetFlow in cybersecurity, exploring its benefits, challenges, and integration with other security tools.

NetFlow's ability to provide detailed insights into network traffic is a critical advantage for cybersecurity. According to Hofstede Tal. (2014), NetFlow data encompasses key information such as IP addresses, ports, and protocols, which are essential for understanding network behaviour and identifying anomalies . This detailed traffic visibility is instrumental in distinguishing normal network activity from potentially malicious behaviour. Anomaly detection is a primary application of NetFlow in cybersecurity. Through statistical analysis and machine learning algorithms, NetFlow data can help establish baseline traffic patterns and identify deviations that may indicate security incidents. Research by Sperotto et al. (2010) highlights the effectiveness of flow-based monitoring in detecting network anomalies, such as DDoS attacks and unauthorized data transfers . The ability to detect such deviations early is crucial for preventing and mitigating cyber threats.

## 2. What Is a Flow in NetFlow?

A flow is a unidirectional series of packets between a given source and destination. In a flow, the same source and destination IP addresses, source and destination ports, and IP protocol are shared. This is often referred to as the 5- tuple. Figure shows an example of a flow between a client and a server.




In Figure, the client (source) establishes a connection to the server (destination). When the traffic traverses the router (configured for NetFlow), it generates a flow record. At the very minimum, the 5-tuple is used to identify the flow in the NetFlow database of flows kept on the device. This database is often called the NetFlow cache. Depending on the version of NetFlow, the router can also gather additional information, such as type of service (ToS) byte, differentiated services code point (DSCP), the device's input interface, TCP flags, byte counters, and start and end times.

Flexible NetFlow, Cisco's next-generation NetFlow, can track a wide range of Layer 2, IPv4, and IPv6 flow information, such as the following:

- Source and destination MAC addresses
- Source and destination IPv4 or IPv6 addresses
- Source and destination ports
- ToS
- DSCP
- Packet and byte counts
- Flow timestamps
- Input and output interface numbers
- TCP flags and encapsulated protocol (TCP/UDP) and individual TCP flags
- Sections of a packet for deep packet inspection
- All fields in an IPv4 header, including IP-ID and TTL
- All fields in an IPv6 header, including Flow Label and Option Header Routing information, such as next-hop address, source autonomous system number (ASN), destination ASN, source prefix mask, destination prefix mask, Border Gateway Protocol (BGP) next hop, and BGP policy accounting traffic index.

NetFlow protocol data units (PDUs), also referred to as flow records, are generated and sent to a NetFlow collector after the flow concludes or expires (times out).

## 3. The NetFlow Cache

There are three types of NetFlow cache:

### 1. Normal cache:

This is the default cache type in many infrastructure devices enabled with NetFlow and Flexible NetFlow. The entries in the flow cache are removed (aged out) based on the configured timeout active seconds and timeout inactive seconds settings.

### 2. Immediate cache:

- Flow accounts for a single packet
- Desirable for real-time traffic monitoring and distributed
- DoS (DDoS) detection
- Used when only very small flows are expected (for example, sampling)

### 3. Permanent cache:

Used to track a set of flows without expiring the flows from the cache. The entire cache is periodically exported (update timer). The cache is a configurable value. After the cache is full, new flows will not be monitored. Uses update counters rather than delta counters.

### 4. Cisco Flexible NetFlow

Flexible NetFlow provides enhanced optimization of the network infrastructure, reduces costs, and improves capacity planning and security detection beyond other flow-based technologies available today. Flexible NetFlow supports IPv6 and Network-Based Application Recognition (NBAR) 2 for IPv6 starting in Cisco IOS Software Version 15.2(1)T. It also supports IPv6 transition techniques (IPv6 inside IPv4). Flexible NetFlow can detect the following tunneling technologies that give full IPv6 connectivity for IPv6- capable hosts that are on the IPv4 Internet but that have no direct native connection to an IPv6 network:

- Teredo
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- 6to4
- 6rd

Flexible NetFlow classification inside Teredo, ISATAP, 6to4, and 6rd was introduced in Cisco IOS Software Version 15.2(2)T. Export over IPv6 was introduced in Cisco IOS Software Version 15.2(2)T, Cisco IOS XE 3.7.0S, and Cisco Nexus Software

Version 4.2.1. Flexible NetFlow tracks different applications simultaneously. For instance, security monitoring, traffic analysis, and billing can be tracked separately, and the information customized per application. Flexible NetFlow allows the network administrator or security professional to create multiple flow caches or information databases to track. Conventionally, NetFlow has a single cache and all applications use the same cache information. Flexible NetFlow supports the collection of specific security information in one flow cache and traffic analysis in another. Subsequently, each NetFlow cache serves a different purpose. For instance, multicast and security information can be tracked separately and the results sent to two different collectors. Figure 4-8 shows the Flexible NetFlow model and how three different monitors are used. Monitor 1 exports Flexible NetFlow data to "Exporter 1." Monitor 2 exports Flexible NetFlow data to "Exporter 2," and Monitor 3 exports Flexible NetFlow data to "Exporter 1" and "Exporter 3."

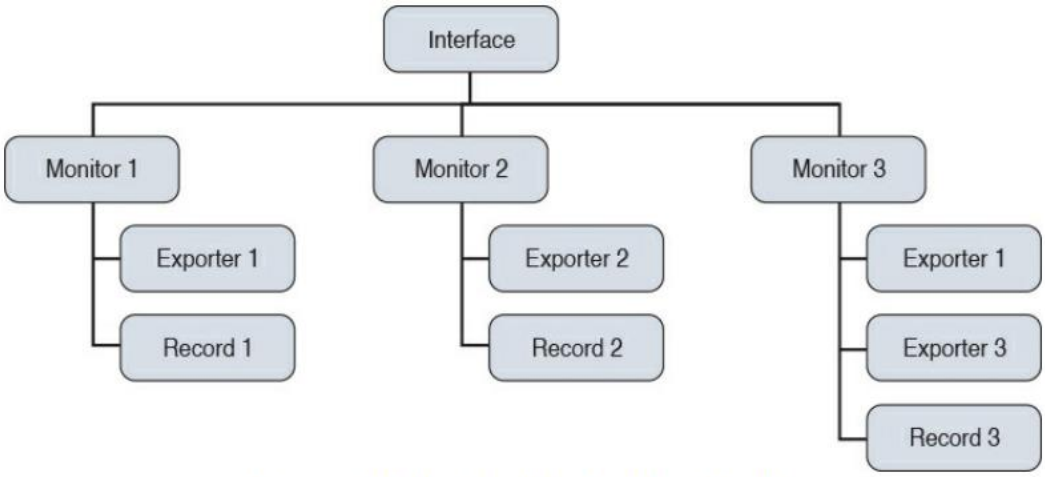



**Figure 4-8** The Flexible NetFlow Model

The following are the Flexible NetFlow components:

- Records Flow monitors
- Flow exporters
- Flow samplers

In Flexible NetFlow, the administrator can specify what to track, resulting in fewer flows. This helps to scale in busy networks and use fewer resources that are already taxed by other features and services.

### 5. Flexible NetFlow Records

Flexible NetFlow records are a combination of key and non-key fields. In Flexible NetFlow, records are appointed to flow monitors to define the cache that is used for storing flow data. There are seven default attributes in the IP packet identity, or "key fields," for a flow and for a device to determine whether the packet information is unique or similar to other packets sent over the network. Fields such as TCP flags, subnet masks, packets, and number of bytes are "non-key fields." However, they are often collected and exported in NetFlow or in IPFIX.

### 6. NetFlow Predefined Records

Flexible NetFlow includes several predefined records that can help an administrator and security professional start deploying NetFlow within their organization. Alternatively, they can create their own customized records for more granular analysis. As Cisco evolves Flexible NetFlow, many popular user-defined flow records could be made available as predefined records to make them easier to implement. The predefined records guarantee backward compatibility with legacy NetFlow collectors. Predefined records have a unique blend of key and nonkey fields that allows the network administrator and security professional to monitor different types of traffic in their environment without any customization.

### 7. User-Defined Records

As the name indicates, Flexible NetFlow gives the network administrator and security professional the flexibility to create their own records (user-defined records) by specifying key and non-key fields to customize the data collection. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow. Flexible NetFlow enables you to capture counter values such as the number of bytes and packets in a flow as non-key fields. Flexible NetFlow adds a new NetFlow v9 export format field type for the header and packet section types. A device configured for Flexible NetFlow communicates to the collector the configured section sizes in the corresponding NetFlow v9 export template fields.

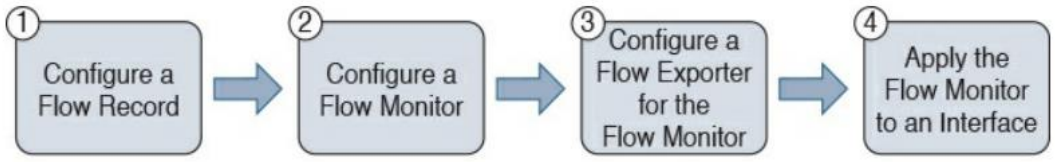
### 8. Table

| Field | Description |
|---|---|
| flowset_id | A FlowSet ID precedes each group of records within a NetFlow v9 data FlowSet. The FlowSet ID maps to a (previously received) template_id. The collector and display applications should use the flowset_id to map the appropriate type and length to any field values that follow. |
| length | This field gives the length of the data FlowSet. Length is expressed in TLV format, meaning that the value includes the bytes used for the flowset_id and the length bytes themselves, as well as the combined lengths of any included data records. |
| record_N through field_M | The remainder of the v9 data FlowSet is a collection of field values. The type and length of the fields have been previously defined in the template record referenced by the flowset_id/template_id. |
| padding | Padding should be inserted to align the end of the FlowSet on a 32-bit boundary. Pay attention that the length field will include those padding bits. |

**Table 4-13** NetFlow v9 Data FlowSet Definitions

### 9. Flexible NetFlow Configuration

The following sections provide step-by-step configuration guidance on how to enable and configure Flexible NetFlow in a Cisco IOS device. Figure shows the configuration steps in a sequential graphical representation.




Flexible NetFlow Configuration steps

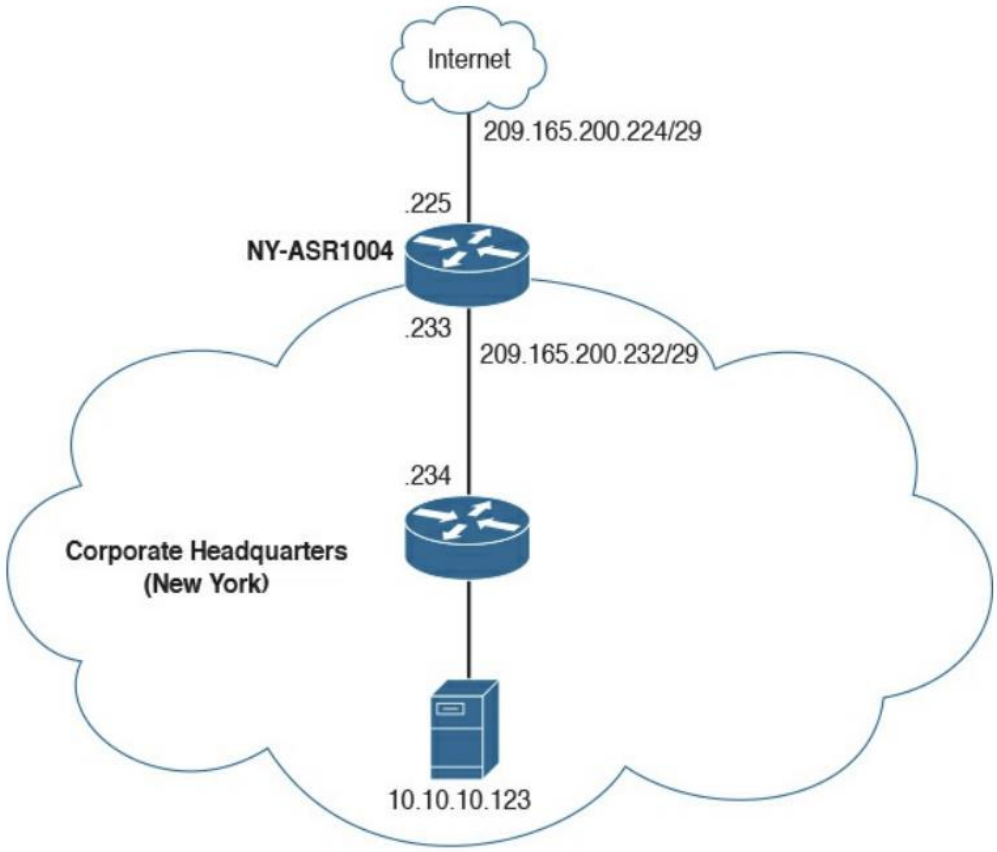
The configuration steps, which are described in detail in the corresponding sections, are as follows: Step 1. Configure a flow record

Step 2. Configure a flow monitor

Step 3. Configure a flow exporter for the flow monitor

Step 4. Apply the flow monitor to an interface

The topology shown in Figure is used in the following examples.




Flexible NetFlow Configuration Exaple Topology

### 10. Flexible NetFlow Key

Fields There are several Flexible NetFlow key fields in each packet that is forwarded within a NetFlow-enabled device. The device looks for a set of IP packet attributes for the flow and determines whether the packet information is unique or similar to other packets. In Flexible NetFlow, key fields are configurable, which enables the administrator to conduct a more granular traffic analysis.

Table 4-15 lists the key fields related to the actual flow, device interface, and Layer 2 services.

| | Flow | Interface | Layer 2 |
|---|---|---|---|
| Fields | Sampler ID | Input | Source VLAN |
| | Direction | Output | Destination VLAN |
| | Class ID | | Dot1q priority |
| | | | Source MAC address |
| | | | Destination MAC address |

**Table 4-15** Flexible NetFlow Key Fields Related to Flow, Interface, and Layer 2

Table 4-16 lists the IPv4- and IPv6-related key fields.

| | IPv4 | IPv6 |
|---|---|---|
| Fields | IP (Source or Destination) | IP (Source or Destination) |
| | Prefix (Source or Destination) | Prefix (Source or Destination) |
| | Mask (Source or Destination) | Mask (Source or Destination) |
| | Minimum-Mask (Source or Destination) | Minimum-Mask (Source or Destination) |
| | Protocol | Protocol |
| | Fragmentation Flags | Traffic Class |
| | Fragmentation Offset | Flow Label |
| | Identification | Option Header |
| | Header Length | Header Length |
| | Total Length | Payload Length |
| | Payload Size | Payload Size |
| | Packet Section (Header) | Packet Section (Header) |
| | Packet Section (Payload) | Packet Section (Payload) |
| | Time to Live (TTL) | DSCP |
| | Options bitmap | Extension Headers |
| | Version | Hop-Limit |
| | Precedence | Length |
| | DSCP | Next-header |
| | TOS | Version |

**Table 4-16** Flexible NetFlow IPv4 and IPv6 Key Fields

Table 4-17 lists the Layer 3 routing protocol–related key fields.

| | Routing |
|---|---|
| Fields | Source or Destination AS |
| | Peer AS |
| | Traffic Index |
| | Forwarding Status |
| | Input VRF Name |
| | IGP Next Hop |
| | BGP Next Hop |

Table 4-18 lists the transport-related key fields.

| | Transport |
|---|---|
| Fields | Destination Port |
| | Source Port |
| | ICMP Code |
| | ICMP Type |
| | IGMP Type (IPv4 only) |
| | TCP ACK Number |
| | TCP Header Length |
| | TCP Sequence Number |
| | TCP Window-Size |
| | TCP Source Port |
| | TCP Destination Port |
| | TCP Urgent Pointer |

**Table 4-18** Flexible NetFlow Transport Key Fields

Table 4-19 lists the multicast-related key fields.

| | Multicast |
|---|---|
| Fields | Replication Factor (IPv4 only) |
| | RPF Check Drop (IPv4 only) |
| | Is-Multicast |

**Table 4-19** Flexible NetFlow Multicast Key Fields

### 11. Flexible NetFlow Non-Key

Fields There are several non-key Flexible NetFlow fields. Table 4-20 lists the nonkey fields that are related to counters, such as byte counts, number of packets, and more. A network administrator can use non-key fields for different purposes. For instance, the number of packets and amount of data (bytes) can be used for capacity planning and also to identify denial-of-service (DoS) attacks as well as other anomalies in the network.

| | Counters |
|---|---|
| Fields | Bytes |
| | Bytes Long |
| | Bytes Square Sum |
| | Bytes Square Sum Long |
| | Packets |
| | Packets Long |
| | Bytes Replicated |
| | Bytes Replicated Long |
| | Packets Replicated |
| | Packets Replicated Long |

**Table 4-20** Flexible NetFlow Counters Non-Key Fields

Table 4-21 lists the timestamp-related non-key fields

| | Timestamp |
|---|---|
| Fields | sysUpTime First Packet |
| | sysUpTime First Packet |
| | Absolute First Packet |
| | Absolute Last Packet |

**Table 4-21** Flexible NetFlow Timestamp Non-Key Fields

Table 4-22 lists the IPv4-only non-key fields.

| | IPv4 Only |
|---|---|
| Fields | Total Length Minimum |
| | Total Length Maximum |
| | TTL Minimum |
| | TTL Maximum |

**Table 4-22** Flexible NetFlow IPv4-Only Non-Key Fields

Table 4-23 lists the IPv4 and IPv6 non-key fields

| | IPv4 and IPv6 |
|---|---|
| Fields | Total Length Minimum |
| | Total Length Maximum |

**Table 4-23** Flexible NetFlow IPv4 and IPv6 Non-Key Fields

## 12. Result and discussion

### Results

The application of NetFlow in cybersecurity has been extensively researched and implemented, yielding several significant outcomes NetFlow provides detailed metadata on network traffic, including IP addresses, ports, and protocols. Studies have shown that this data is crucial for mapping network behavior and identifying normal vs. abnormal traffic patterns .

### Discussion

The findings from various studies highlight the substantial benefits of utilizing NetFlow in cybersecurity, though several challenges and limitations remain. The detailed insights provided by NetFlow data are invaluable for maintaining situational awareness of network activity. This visibility is essential for detecting and mitigating security threats promptly. By establishing and monitoring baseline traffic patterns, NetFlow helps in the early detection of anomalies. This proactive approach is crucial in preventing potential breaches and mitigating the impact of ongoing attacks. The ability to analyze historical network traffic aids in a thorough investigation of security incidents, enabling faster and more effective responses.

## Conclusion

NetFlow, as a network protocol for collecting and monitoring IP traffic data, has proven to be a powerful tool in enhancing cybersecurity measures. Its ability to provide detailed insights into network traffic patterns, facilitate anomaly detection, and support incident response makes it indispensable for modern network security strategies.

## References


1. https://www.ciscopress.com/store/ccna-cyber-ops-secops-210-255-official-cert-guide-9781587147036
2. **Hofstede, R., et al.** (2014). "Flow monitoring explained: From packet capture to data analysis with NetFlow and IPFIX." *IEEE Communications Surveys & Tutorials*, 16(4), 2037-2064. doi:10.1109/COMST.2014.2321898
3. **Sperotto, A., et al.** (2010). "An overview of IP flow-based intrusion detection." *IEEE Communications Surveys & Tutorials*, 12(3), 343-356. doi:10.1109/SURV.2010.032210.00054

4. **Zuech, R., Khoshgoftaar, T. M., & Wald, R.** (2015). "Intrusion detection and Big Heterogeneous Data: a Survey." *Journal of Big Data*, 2(1), 3. doi:10.1186/s40537-015-0013-4
5. **Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K.** (2014). "Network anomaly detection: methods, systems and tools." *IEEE Communications Surveys & Tutorials*, 16(1), 303-336. doi:10.1109/SURV.2013.052213.00046
6. **Trammell, B., & Boschi, E.** (2011). "An introduction to IP flow information export (IPFIX)." *IEEE Communications Magazine*, 49(4), 89-95. doi:10.1109/MCOM.2011.5741145
7. **Brownlee, N., & Zander, S.** (2010). "Improved flow-based techniques for Internet traffic classification." *IEEE Communications Surveys & Tutorials*, 12(1), 1-12. doi:10.1109/SURV.2010.021510.00019
8. **Dainotti, A., et al.** (2012). "Issues and future directions in traffic classification." *IEEE Network*, 26(1), 35-40. doi:10.1109/MNET.2012.6135854
9. **Callado, A., et al.** (2009). "A survey on Internet traffic identification." *IEEE Communications Surveys & Tutorials*, 11(3), 37-52. doi:10.1109/SURV.2009.090303