Network as a Security Sensor

Threat Defense with Full NetFlow

Network Security and Netflow

Historically IT organizations focused heavily on perimeter network security to protect their networks from cyber-attacks. Protection at the perimeter edge works well for data moving in and out towards the protected assets. However, recent breaches have shown that the perimeter security alone isn’t sufficient to combat the advanced persistent threats. With the advent of BYOD, Cloud and the Internet of Things (IOT), data no more resides only on the key servers and access to the network is no more granted in a restricted fashion. To protect the network against the emerging threats IT organizations need intelligent solutions that is pervasive, behavior-based and complimentary to the current zone-based security solutions. One such solution is to leverage the network infrastructure itself to function like a sensor. This is done by activating the network to collect IP traffic flows and deploy anomaly detection system based on network behavior analysis (network traffic monitoring) to detect suspicious traffic flows, policy violations and compromised endpoints by analyzing network traffic for unusual behavior, events or trends.

Network Behavior Analysis

Organizations are fundamentally changing the way they deliver technology to their employees and provide access to critical data. Access to critical data on mobile devices, either on or off the corporate network is a common practice now. Virtualization and cloud computing are fundamentally changing how data centers are built and where the data resides, making it far more challenging to secure critical data. There is an increasing need to provide visibility, control, and threat prevention for these evolving, highly mobile, distributed, and dynamic computing environments. New cloud-based and mobile technology architectures break assumptions about when certain devices are on the network and where they should be connecting from, and they dramatically complicate the use of network security controls. First-generation network security tools do not provide adequate visibility to factor in
dynamic network topologies. The increasing level of sophistication and customization of malicious attacks are forcing organizations to implement stringent security measures in their networks to alert them of any potential security breach incident before it occurs. As such Network behavior analysis (NBA) or Network traffic monitoring is fast becoming necessary part of any network along with anomaly detection systems to ensure comprehensive network security.

Security analysts recommend that IT organizations should deploy Network behavior analysis (NBA) solution in addition to the perimeter based security solutions such as firewalls and intrusion prevention system (IPS) in their networks as part of security and threat protection strategy. Behavior analysis based systems are often able to detect security threats such as malware, viruses and botnets against which other security tools many a times are ineffective. Its is a mechanism to enhance the security of a network by monitoring traffic and detecting unusual actions, events or trends in the network traffic flows from normal operation.

There are various mechanisms to capture network traffic flow information from the network and most of these options are already available on the network infrastructure that are deployed in an IT network today. In order to detect and mitigate security attacks , IT organizations can activate one or more of these technologies that monitor applications and network flow data collected from the network. Some of these include:

- **Network capture solution**: Capturing network packets for all flows within the network can be accomplished by deploying sniffers or network TAP’s and redirecting this traffic to a security analyzer. While this method provides full visibility into all flows that reside in the network it can be really expensive to deploy, difficult to manage and retain transactions for long. Appying network TAP’s at various parts of the network can be significantly expensive in terms of the cost of network TAP’s, packet capture software and security analyzer to correlate all the packet capture to identify and mitigate security attacks.

- **Sampled flow export (packet capture) solution**: Sampled packet captures from network devices can be accomplished by sending "sampled" packet capture from network elements to a dedicated security analyzer/collector. While this solution can be helpful for capacity planning and gaining traffic/application visibility but it falls short for when used for real-time threat mitigation. When network transactions are analyzed in a sampled manor, most of the realtime transactions go unnoticed.

- **Full flow-export based solution**: IP flow monitoring (NetFlow) coupled with security focused NetFlow collectors like Lancope’s StealthWatch quickly identify unusual activities and anomalous behavior. Full NetFlow provides un-sampled accounting of all network activity on an IP flow enabled interface and is useful in event correlation and data analytics. The key here is to collect un-sampled flows as it helps reduce false positives compared to sampled packet capture solutions. In addition, having full flow visibility also enables this solution to identify slow network scanning and atomic attacks which would not have been identified by traditional security solutions.

Implementing network TAP’s can be quite an expensive solution and doesn’t scale very well in a large enterprise network. The Flexible NetFlow based NBA is the best mechanism among these options that provides deep and broad visibility into unknown devices, unusual traffic patterns, and unexpected behavior. Cisco IOS Flexible NetFlow is a powerful information source for every network conversation and captures each and every network conversation over an extended period of time. Enabling NetFlow on network access layer devices can activate the network as a sensor and provide un-sampled accounting of all network activity to a security focused NetFlow collector for anomaly detection and mitigation.
Types of Flow Export Technologies:
There are mostly two types of flow export technologies that are predominant on network elements today: sFlow and Netflow. Both of these flow export technologies were historically developed for providing monitoring and troubleshooting capabilities within the network. This white paper will discuss each of these technologies, their evolution and relevance for designing a threat defense system in more detail starting with Netflow.

Netflow Overview
NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. It was originally invented by Cisco as a packet switching technology for Cisco routers. The simple idea behind NetFlow was that the first packet of a flow would create a NetFlow switching record on the switch or router and subsequently this record would then be used for all later packets of the same flow, until the expiration of the flow. Only the first packet of a flow would require an investigation of the route table to find the most specific matching route.

The flow information on the box can be exported and today its used for network performance analysis and behavioural analytics for security. The flows do not contain the actual packet data itself but rather the metadata for the communications. It is a standard form of session data that details the who, what, when, and where of network traffic. It is similar to the call records in a phone bill, but in realtime. Every network transaction typically gets two flows, one in each direction.

Figure 1. NetFlow Overview

<table>
<thead>
<tr>
<th>Flow Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
</tr>
<tr>
<td>10:20:12.221</td>
</tr>
<tr>
<td>10:20:12.871</td>
</tr>
</tbody>
</table>

Figure 2. A single NetFlow record provides a wealth of information
NetFlow operations:

When the switch or router sees IP traffic passing through an interface it captures the flow information and stores it in a cache on the switch or router. This piece of information is called NetFlow and the cached data is exported periodically based on the active and inactive timeouts. NetFlow captures flow information of all IP traffic conversations that pass through an interface and reports the entire interface traffic. The NetFlow information or record can be exported to a NetFlow Collector in various formats, these are called export versions. The most popular and widely used NetFlow export versions are version 5 and 9. Among these two versions, the most common format used is NetFlow export version 5 but version 9 is the latest format and has some advantages for key technologies such as security, traffic analysis and multicast.

The process of NetFlow data reporting which includes capturing IP flows, aggregating those on the switch or router, exporting them to a NetFlow collector is explained in the following steps below:

- NetFlow is configured to capture flows to the NetFlow cache
- NetFlow export is configured to send flows to the collector
- The NetFlow cache is searched for flows that are aged (through active, inactive timers and Cache limits) or terminated (via TCP RST and FIN flags) and these are exported to the NetFlow collector server
- Approximately 20-25 flows are bundled together and typically transported in UDP format to the NetFlow collector server
- The NetFlow collector software creates real-time or historical reports from the data

Figure 3. Netflow Agent, Collector and Analyzer
Netflow Evolution towards standards based IPFIX

NetFlow has evolved over the years resulting in several versions of NetFlow record. The table below provides information on three NetFlow versions that are in use currently. NetFlow v9 is the most recent future proof version. It is template based with an extensible design to the record format, a feature that allows future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. This means it can be extended to add support for new protocols by modifying the existing template.

Table 1. Netflow Version details

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v5</td>
<td>Most common version, available (as of 2009), but restricted to IPv4 flows.</td>
</tr>
<tr>
<td>v9</td>
<td>Template Based, available on most of the recent routers and switches. Mostly used to report flows like IPv6, MPLS, or even plain IPv4 with BGP nexthop.</td>
</tr>
<tr>
<td>IPFIX</td>
<td>IPFIX stands for &quot;IP Flow Information eXport&quot; and is an IETF standard based on NetFlow v9.</td>
</tr>
</tbody>
</table>

NetFlow v5 is limited to the IPv4 flows and also the fields that can be exported using this version are limited.

NetFlow v9 is the most recent version and offers several benefits over the older formats. NetFlow v9 template allows to define what to send in a record, it is possible to send less details and ultimately squeeze more flows into a v9 datagram.

IPFIX is the standards based evolution of NetFlow and considers a flow to be any number of packets observed in a specific timeslot and sharing a number of properties, e.g. "same source, same destination, same protocol". IPFIX allows the sending device to use user-defined data types in the messages through the help of special templates. IPFIX is a push protocol where each sender will periodically send IPFIX messages to configured receivers without any interaction by the receiver. IPFIX prefers the Stream Control Transmission Protocol (SCTP) as its transport layer protocol, but also allows the use of the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).
Flexible Netflow and IPFIX

Flexible NetFlow (FnF) is the next generation IP flow monitoring technology from Cisco that introduces two new concepts to flow monitoring. First it allows the use of templates and second it allows user to look deep inside the packet and select custom fields to monitor. Typically NetFlow tracks these fields in an IP flow namely IP addresses, ports, protocols, TCP Flags. Flexible NetFlow allows the user to select almost all the fields from the IP header, all types of TCP flags and other information too for example VLAN tags and URLs.

NetFlow typically tracks IP information such as IP addresses, ports, protocols, TCP Flags and based on this information most security systems look for anomalies or changes in network behavior to detect security incidents. Flexible NetFlow allows the user to track a wide range of IP information including all the fields in the IPv4 header or IPv6 header, a variety of individual TCP flags and it can also export sections of a packet. The information being tracked may be a key field (used to create a flow) or non-key field (collected with the flow). The user has the ability to use one NetFlow cache to detect security vulnerability (anomaly detection) and then create a second cache to focus or zoom in on the particular problem.

NetFlow v9 came first and the IPFIX RF 5101 and RFC 5102 dervied capabilities from the Netflow v9 RFC. IPFIX lists an overview of the “Information Element identifiers” that are specified in Section 5 of the RFC and are compatible with the “field types” used by NetFlow v9. IT administrators can configure Netflow v9 on Cisco devices and export it with IPFIX format for standards based approach. Key advantages to IPFIX export include:

- IPFIX allows a vendor ID to be specified whereby the vendor can include proprietary information
- IPFIX allows for variable length fields useful for exporting URLs.

Advantages of Flexible netflow (v9)/IPFIX over traditional netflow:

- Flexibility, scalability, aggregation of flow data beyond traditional NetFlow.
- The ability to monitor a wider range of IP packet information from layer 2 to 7
- Enhanced network anomaly and security detection
- User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network behavior
- Convergence of multiple accounting technologies into one accounting mechanism

Netflow Use:

NetFlow has extensive usage in the network industry and is used for multiple objective ranging from network capacity planning to network analytics to security forensics. Listed below are some of the main use cases for NetFlow data:

- **Network visibility** – by allowing NetFlow records export to a NetFlow collector it helps in driving visibility into the network traffic and behavior. Helps identify network utilization, helps in network capacity planning.
- **Capacity Planning** – measuring traffic flow and Bandwidth usage
- **Traffic Analysis** – Application flow monitoring.
- **Security Vulnerability detection** – understanding the network traffic helps in detection of new IP applications and security vulnerabilities.

- **Segmentation policy validation** – With netflow the network segmentation policies can be monitored for compliance. Any unexpected transactions happening between the segments of the network can be detected using Netflow analysis.

- **Network reconnaissance detection** - detecting TCP and UDP scans in various forms (including unusual flag configurations), stealth TCP scans, or the reuse of ports, low and slow scans, and ICMP scans.

- **Data loss prevention**: Granular traffic flow visibility along with other security measures can be used to prevent persistent, widespread attacks against customer data, trade secrets, intellectual property, email, or financial data.

- **Internally spreading malware**: Netflow can provide visibility and offer effective ways to establish a baseline for host network behavior, monitor which internal devices a host is communicating with, and apply the behavior and communication to a set of rules and policies to determine if malware is spreading.

**sFlow Overview**

sFlow aka "sampled flow", supported on selected Cisco switches (Like Nexus 3000 series) and on non Cisco platforms provides a mean for exporting truncated packets along with interface counters. sFlow has evolved to become an industry standard for packet export at Layer 2. The current version of sFlow is v5.

sFlow is a packet sampling technology. sFlow captures 1 in "n" packets (where "n" is the sampling rate) from the interface traffic, copies the first "x" bytes (the default is 128 bytes for sFlow v5) of the sampled packet and exports them in user datagram packets (UDP) packets called sFlow datagrams. The first "x" bytes cover the relevant header data required to construct information about the traffic. But sFlow can miss IP flows, due to its focus on packets. When packets are captured for analysis, it is not necessary that the sampled packets represent every IP flow (conversation) that passed through an interface. IP flows whose packets were not collected will not be accounted for, resulting in some visibility gaps in network conversations.

Figure 4. sFlow packet
sFlow operations

sFlow system consists of multiple devices performing two types of sampling: random sampling of packets or and time-based sampling of counters. The sampled packet/operation and counter information, referred to as flow samples and counter samples respectively, are sent as sFlow datagrams to a central server running software that analyzes and reports on network traffic; the sFlow collector.

sFlow randomly samples network packets and sends these samples to an outside sFlow Collector that functions as the monitoring station. For the purpose of monitoring actual usage of various applications and statistical analysis of network utilization, a uniformly distributed sampling method such as sFlow is considered accurate and robust enough to cope with high bandwidth services.

sFlow frames sent from the sFlow supporting Network Elements to the sFlow collector are UDP packets destined to the specified host and UDP port (by default, this is port number 6343). The lack of reliability in the UDP transport mechanism does not significantly affect the accuracy of the measurements obtained from an sFlow agent. Each sFlow datagram provides information about the sFlow version, the originating device’s IP address, a sequence number, the number of samples it contains and one or more frames and/or counter samples.

Similar to sFlow, NetFlow also collects traffic frames and later exports a statistics summary of the analyzed flow via a standard NetFlow record which is also a set of UDP frames (usually destined to port 2055). The Netflow system is also comprised of a NetFlow client (or Exporter) and a NetFlow Collector, typically, a server that collects and does the actual traffic analysis (mostly the analyzer is a separate server).

Unlike Netflow which is mostly done in hardware, sFlow uses sampling to achieve scalability as it mostly establishes a burden on CPU and memory footprint for devices that are exporting the sampled packet. It is a good tool for troubleshooting and capacity planning but not so much for security, given that it only sends part of the sampled packet and does not have a holistic view of the all the flows in the network which is required to detect malicious behavior and malware/botnets that might exist in the network.

Comparing sFlow versus Netflow

<table>
<thead>
<tr>
<th>Particulars</th>
<th>NetFlow</th>
<th>sFlow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet capture</td>
<td>Does not capture any packets.</td>
<td>Copies all packets and samples 1 in N to send to collector</td>
</tr>
<tr>
<td>Protocol support</td>
<td>Layer 2, IP and IPv6</td>
<td>Network layer independent</td>
</tr>
<tr>
<td>Configurable packet fields</td>
<td>Flexible NetFlow – user configurable field option (templates)</td>
<td>Fixed protocol information fields</td>
</tr>
<tr>
<td>Flow records</td>
<td>Supports IPv4, IPv6 flow records for all traffic</td>
<td>No Flow records created, copies first N bytes of the packet</td>
</tr>
<tr>
<td>Hardware acceleration</td>
<td>Yes, Flow records are created in hardware</td>
<td>No hardware acceleration. Packets</td>
</tr>
</tbody>
</table>

Table 2.  sFlow sampling rate

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>Sampling Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>1 in 200</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>1 in 500</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>1 in 1000</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>1 in 2000</td>
</tr>
<tr>
<td></td>
<td>with no impact to data plane</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Industry standard</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Flow timestamp (flow start and finish times)</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet rates (no of packet in the flow)</td>
<td>Yes</td>
</tr>
<tr>
<td>Byte count (total no of bytes in the flow)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

NetFlow and sFlow are fundamentally different. The former is a record of traffic flowing through the network which can be done for all transactions (Full NetFlow) or on a sampling rate (Sampled NetFlow), while the later is a sampling only technology in which the switch/router samples a fixed length of information randomly from one in “N” packets.

In summary the benefits of Netflow include:

- **Efficiency:** Since Netflow is implemented in hardware at wire speed, a high degree of efficiency is achieved.

- **Accuracy:** Full netflow provides accurate details on the every network transactions while sampled flow methodologies don’t.

  Users can obtain detailed information from Layer 2 through Layer 7 on all flows. Protocols such as IP and MPLS, are supported.

- **Scalability:** Since Netflow has no impact to network device data plane, it is supported across all speeds, 1GE, 10GE, 40GE and 100GE interfaces. The technology also scales to monitor tens of thousands of flows over several hundred ports.

- **Deployment ease.** Netflow can be easily deployed on existing networks, and is easy to configure. It has among the most widely available flow-record collector software.

- **Real time:** Since Netflow is done in hardware, changes in flow rates are reflected in real time in the flow statistics.

- **Cost Effective:** Since Netflow based solution doesn’t involve network TAPs or involve inline methods for anomaly detection, it’s the most cheapest methods to implement intrusion detection.

**Anatomy of a typical data breach**

Any enterprise network that is connected to the Internet today is a target for cyber attack. A majority of the enterprises that were subject to data breaches had good perimeter controls, however they were ineffective in detecting the data theft. Most of the current security practices can be compared to that of an egg-shell, which is hard on the outside while softer inside. Which means that once the internal assets are compromised, its easy to get control in to the network and steal the data of interest.

**Figure 5.** Life cycle of a typical cyber attack
To be able to effectively protect the network from the hackers, it's important to understand their modus operandi. Most cyber thefts involve the following 5 stages:

1. **Infiltration and Backdoor establishment** - The attacker through emails, file transfers or system vulnerabilities enters and inserts malware into the enterprise network. The initial infection sets up Command and control access to the internet server operated by the attacker and additional instructions or malicious code is sent from there.

2. **Reconnaissance and Network Traversal** - It is very likely that the compromised computer does not contain the targeted data. The next logical step that the attacker employs is to discover the network topology and the servers where the critical data are stored. The attacker performs various scanning and exploration activities during this stage.

3. **Exploitation and Privilege Elevation** - Once the attacker has identified the critical server(s), attempts will be made to escalate the access privileges to it. Which is done either by kernel level code execution or by impersonating identity of authorized users.

4. **Staging and Persistence** - The compromised data which could be in large volumes will be temporarily copied to an on-premise staging server. Data from various internal sources may be persistently copied to this server over a period of time.

5. **Data Exfiltration** - The malware then compresses the data on the staging server and exfiltrates it off the network to the Command-and-Control (C&C / C2) server. The attacker clears the traces of theft and later monetizes the stolen data.

**Cyber Threat Defense with NetFlow**

The cyber breach life-cycle clearly depicts why perimeter-only approach may not be effective to defend security threats, because most of the activity happens in the inside of the network and many times these activities appear legitimate. Although full packet capture everywhere in the network is technically possible and provides undeniably valuable information in the event of a security incident, it's simply not feasible. One of the simplest means to enable the Enterprise network as a “Sensor” is to activate full flexible NetFlow in the network and analyze the network...
transactions centrally. Such a security system can detect and alarm various malicious activities in the network, some of them are:

**Figure 6. Netflow based anomaly detection**

- **Network Scanning** - The context rich, NetFlow records provide insights into various network transactions including network scanning activities like TCP/UDP port scans and Ping traces in realtime.

- **Denial of Service** - Netflow based analysis can detect and report Denial of Service attacks such as TCP half open, ICMP and UDP port flooding.

- **Host Reputation Change** - Every host in the enterprise network is tracked by NetFlow Analyzer and is given a reputation score. When the hosts behave suspiciously, appropriate alarm is triggered and the admin is notified of the change.

- **Botnet Detection** - Botnets essentially makes connection to the Command and Control servers and download malicious content. NetFlow analyzer can track and report these connections to the blacklisted servers.

- **Fragmentation Attack** - NetFlow records can be customized to report IP Fragmentation ID, Fragment offset, and the Packet length to the Analyzer. The Analyzer can monitor and flag IP fragmentation exploits.

- **Worm Propagation** - NetFlow analyzers like Lancope StealthWatch system can track worms about where they exist and where it is likely to go next. The Worm Tracker can visually graph the spread of a worm or virus throughout the network from node to node, providing instant visibility into the scope and impact of an outbreak. This way, malware propagation can be halted within hours instead of weeks.

- **Data Exfiltration** - Most of the data thefts happen in large volumes but over a longer duration. Netflow analysis can detect a user that is downloading more data internally than they normally do which can be a signal to the security administrator to look at the forensic flow data contained in Analyzer to see who that host has talked to and how they were talking.
Segmentation Policy Violation - In many organizations, network segmentation has been a "set it and forget it" effort, which once done is almost immediately out of date. Netflow analysis provides visibility into every network transaction and any undesirable communications can be seen and controlled immediately.

Netflow Analysis and Attack Continuum

The industrialization of hacking combined with the any-to-any challenge have profoundly changed how we protect our systems, driving us to think about a new approach to cybersecurity. Its not about “if” an attacker gets in, its about "when". Security solutions needs to be evolved from a point-in-time approach to a continuous model that addresses the full attack continuum before, during and after an attack.


NetFlow based analysis plays an important role in each of the three phases of the attack continuum.

**Figure 7.** Network as a Sensor, Before, During and After

**Before an Attack:** NetFlow based security system baselines the network to understand what is considered as the “normal” traffic pattern. The baselining happens on various parameters like, daily / weekly pattern, upload and download limits per host / per segment and so on. The flow baseline is very useful to detect deviations which most of the time is due to malware activities. Also the netflow based traffic analysis helps the security administrator understand the traffic pattern before enforcing limits or restrictions on them.

**During an Attack:** Once the network is baselined, its easy to detect anomalies. An unexpected traffic pattern or an abnormal upload event to unknown destination(s) would provide insight into a probable malware activity in the network. As discussed in the previous section, there are a numerous cyber threat activities that the NetFlow analyzer can detect and report. A solution like Lancope StealthWatch system comes with several threat event definitions along with a cloud based feed for information on the new C&C server in the internet. Cyber threat defense solutions build on adaptable baselining of the network and sensing anomalies based on that baseline helps defend the businesses from day-0 attacks.

**After an Attack:** Any good security solution should offer for detailed retrospective studies. The lessons learnt after an attack is important to fine tune the security policies and close the loop by solidifying the infrastructure to defend before an attack. Compared to any other data retention methodologies, NetFlow records can be retained for months and years, because of its abstracted nature. In case of an incident, these stored flow information are very handy in tracking back to the attack sequence; source of attack, date of inception, attack traversal and its impact.
Threat Defense solution with Flexible Netflow and Lancope StealthWatch

The solution has two main components: Netflow record sending devices (called Netflow exporters) and Lancope® StealthWatch® System.

- **NetFlow Exporters**: An exporter contains network layer and transport layer details for the NetFlow export packet. The exporter includes information such as, Export destination IP address, Source interface, UDP port number (where the collector is listening for NetFlow packets) and Export format
  - **Flow**: NetFlow defines a flow as a unidirectional sequence of packets that arrive on the same interface of a switch and have the same source IP address, destination IP address, Layer 3 or 4 protocol, TCP or UDP source port number, TCP or UDP destination port number, and type of service (ToS) byte in their TCP, UDP, and IP headers, respectively. Flexible NetFlow optimizes the network infrastructure, reducing operation costs and improving capacity planning and security incident detection with increased flexibility and scalability.
  - **Flow record**: A flow record is created for each unique flow that passes through a NetFlow-enabled device. The information in a flow record expresses key details of the packet header, along with other statistical information such as the number of packets or bytes.
  - **Active timeout**: If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow). This age out process allows the monitoring application that is receiving the exports to remain up to date. By default this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements. The best practise recommendation for most deployments is “60” seconds.
  - **Inactive timeout**: If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected.

- **Lancope® StealthWatch® System**: The Lancope StealthWatch system, available through Cisco, is a purpose-built, high-performance network visibility and security intelligence solution. Through the collection, aggregation, and analysis of NetFlow data, along with other contextual data sources such as identity data from Cisco ISE, system-specific data such as syslog and Simple Network Management Protocol (SNMP), and application data via NBAR2 and Cisco AVC, the Lancope StealthWatch system helps security operations staff gain real-time situational awareness of all users, devices, and traffic on the network.

The solution is composed of two core components: the StealthWatch® Management Console and one or more StealthWatch® FlowCollectors. Additional optional components include a StealthWatch® Flow Sensor and a StealthWatch® Flow Replicator.

- **StealthWatch Flow Collector**: Serves as a central collector for flow data generated by Netflow-enabled devices. The StealthWatch Flow Collector monitors, categorizes, and analyzes network traffic to create comprehensive security intelligence at both the network and host level.
- **StealthWatch Management Console**: Manages, coordinates, and configures all StealthWatch appliances to correlate security and network intelligence across the enterprise. Retrieves authenticated session information from the Cisco ISE to correlate flow and identity.
NetFlow agent running on network devices collect unsampled flow data from each interface and sends this information in the form of flow records to a NetFlow collector. The Management console focused on network security and forensics, analyses the flows in the collector. The management console can get additional feeds such as user and device identity from Cisco ISE or Windows Active directory (User context only), Syslogs, SNMP data, etc, analyzes the flow records to perform behavioural analysis.

**Enabling Netflow on access layer switches:**

NetFlow agent can be configured on any NetFlow capable device in the network. These could be edge routers, firewalls, core switches, distribution layer switches or the access layer switches. Depending upon the purpose of NetFlow data collection it can be enabled in the appropriate locations on the network. For example if the desired goal is to do network capacity planning in the core layer enabling NetFlow agents on the core switches would be good enough to capture the IP flows traversing through the network core to determine the traffic pattern. However for security analytics, network forensics and attack detection NetFlow should be enabled in the access layer switches so that it could collect NetFlow records for all possible IP flow traffic in the network. Distribution layer or core layer switches will surely miss those IP flow records that are generated by network traffic between directly attached hosts on the access layer. Enabling NetFlow agent on every access layer switch in the enterprise network provides the most detailed and precise information to establish a network baseline for:

- Application and network usage – provides traffic information down to the host level without missing details of workstation-to-workstation (east west) communication at the access layer
- Network productivity and utilization of network resources – gives bandwidth usage details not only for aggregate uplink downlink bandwidth but individual port usage
- The impact of design changes to the network – can be tracked quickly and mitigated faster with network visibility down to the endpoint host level
• Network anomaly and security vulnerabilities – compromised hosts can be tracked faster with access layer NetFlow information, any abnormal traffic activity at the individual port level can be noticed now
• Long term compliance issues – It becomes easier to track non compliant hosts on the network and these could be quarantined to avoid further compliance issues on the network.

Figure 9. Traffic coverage by NetFlow based on place in the Network

Enabling NetFlow at the access layer has several benefits as we discussed. This is very helpful to the network administrators to understand who, what, when, where, and how network traffic is flowing. When the network behavior is understood, it can provide an audit trail of how the network is utilized. This increased awareness reduces vulnerability of the network as related to outage and allows efficient operation of the network.

Solution Performance and Scaling:

When deploying this solution, it is important to select hardware and software that will provide the appropriate performance for your network and will scale to your specific needs. The following tables provide key information needed for selecting the right components based on your individual network requirements:

NetFlow Cache Size Limitations on Cisco Devices

Table 4. NetFlow Cache Size Limitations on Cisco Devices

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
<th>Cache Size (flows)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3850, 3650</td>
<td>All models of Catalyst 3850 and 3650</td>
<td>32,000</td>
</tr>
<tr>
<td>Catalyst 4500E Series</td>
<td>Supervisor 8E</td>
<td>128,000</td>
</tr>
<tr>
<td></td>
<td>Supervisor 7L-E</td>
<td>128,000</td>
</tr>
<tr>
<td>Catalyst 6500 Series</td>
<td>Supervisor 2T</td>
<td>512,000</td>
</tr>
<tr>
<td></td>
<td>Supervisor 2TXL</td>
<td>1 million</td>
</tr>
</tbody>
</table>
Netflow or sFlow for threat defense?

A sFlow system consists of multiple devices performing two types of sampling: random sampling of packets or application layer operations, and time-based sampling of counters. Based on a defined sampling rate, an average of 1 out of n packets/operations is randomly sampled. Selecting a suitable packet sampling rate is an important part of configuring sFlow on switch. Typically sFlow is configured to sample 1 in 2000 packets on a 10Gbps links that should work well for general traffic monitoring in most networks. Sampling at the suggested rate in the table above means more than 99% of the traffic is ignored.

Generally this is not a problem when the sample data is used for network capacity planning or traffic engineering tasks. However when packets are captured for security analytics, it is not necessary that the sampled packets represent every IP flow (conversation) that passed through an interface. Security analytics requires analysis of all IP flows in detail to detect any unusual network activity that could be an intrusion. For this, NetFlow is a better choice for network anomaly detection, due to its ability to capture all conversations. sFlow too may be used for anomaly detection, but the chance of it missing a critical flow is high because of its sampling nature.

Any IP flow export protocol that is being used for cybersecurity needs to meet these two requirements

- Generate data by looking at all packets on the wire
- Able to customize what data to look at and report

The choice is not just limited to a selection between sampled flow (sFlow) or unsampled NetFlow rather it is a question of which IP flow protocol can provide customized flow record data with user defined fields that might be of significant use for security analytics purposes. Flexible NetFlow (FnF) fares even better as FnF is template based and also supports new technologies like IPv6 traffic, MPLS labels, multicast traffic, media access control addresses, VLAN identification, jitter and round-trip time of media traffic.

While sFlow can be helpful for capacity planning and gaining traffic/application visiblility but it falls short for providing a holistic security solution due to the following reasons:

- Potentially higher false positives as this solution only exports “sampled” packets which can often appear one sided and wrongly flag legitimate application data. Being based on sampled packets, these flow records often appear one sided and flag data isn’t guaranteed,
- Slower Network scanning attacks cannot be detected: Traditional network scanning attacks done by “traditional worms” can be identified by sampled packet capture solutions but as these attackers have become more sophisticated they tend to make network scanning attacks to be slower and more methodical which allows these attacks to evade detection by sampled packet capture solutions.
- Atomic attacks: Evolving malicous code attacks which only send a single packet make it impossible to be detected with sampled packet capture solutions like sFlow. While flow sampling is a valid method for network management use cases sampling for the sake of security leaves too much in question.

Full flow-export based solution: IP flow monitoring (NetFlow) coupled with security focused NetFlow collectors like Lancope’s StealthWatch quickly identify unusual and suspect activity and anomalous behavior. Full NetFlow provides un-sampled accounting of all network activity on an IP flow enabled interface and is useful in event correlation and data analytics. The key here is to collect un-sampled flows as it helps reduce false positives compared to sampled packet capture solutions. In addition, having full flow visibility also enables this solution to identify slow network scanning and atomic attacks which would not have been identified by other security solutions. Using full flow export technologies like Netflow on network elements along Stealthwatch solution provides the best in class solution to detect and mitigate the evolving cyber attacks.

Flexible NetFlow (FnF) configuration for threat defense
Configuring Flexible NetFlow involves 4 major steps:

1. Create “Flow Record” – Define what data from the transactions to be picked to create a flow
2. Define “Flow Exporter” – Configure where and how to send the flow records
4. Apply the “Flow Monitor” – Enable flow monitoring on desired interface / VLAN / SSID

Figure 10. Configuring Flexible NetFlow

This section provides step-by-step configuration of Flexible NetFlow on a IOS based switch towards threat mitigation solution to send records to Lancope StealthWatch collector.

**Step 1.** Configure a user defined “flow record” to match specific fields in the packet. The “match” statements indicate that it is a key field and the collect keyword is used to identify the non-key field or information added to the flow and exported with the flow. In this particular example, the flow record is configured to match IPv4 source, destination IP, L4 source and destination ports. In addition to this the timestamp and byte, packet counters are also sent.

```
Switch# configure terminal
Switch(config)# flow record my-flow-record
Switch(config-flow-record)# description Collect Flow Data
Switch(config-flow-record)# match datalink mac source address input
Switch(config-flow-record)# match ipv4 tos
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport source-port
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match interface input
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# collect transport tcp flags
Switch(config-flow-record)# collect interface output
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect counter packets long
Switch(config-flow-record)# collect timestamp absolute first
Switch(config-flow-record)# collect timestamp absolute last
Switch(config-flow-record)# collect counter bytes layer2 long
```
Step 2. Define “flow export” destination (collector IP address) and destination port number

```plaintext
Switch(config)# flow export my-flow-export
Switch(config-flow-exporter)# destination <IP address of Flow Collector>
! {flow-collector IP address}
Switch(config-flow-exporter)# transport udp 2055
! {The UDP number of the Flow collector}
Switch(config-flow-exporter)# source <interface>
! {source IP to use to send flows to the Flow collector}
Switch(config-flow-exporter)# template data timeout 60
! {frequency of template exchange with FC}
```

Step 3. Configure a flow monitor and associate the flow record and flow export. Attach the flow monitor to the interface to track input (ingress) traffic

```plaintext
Switch(config)# flow monitor my-flow-monitor
Switch(config-flow-monitor)# record my-flow-record
Switch(config-flow-monitor)# exporter my-flow-export
Switch(config-flow-monitor)# cache timeout active 60
```

Step 4. Apply the “flow monitor” to Layer-2 / Layer-3 interface, SVI, VLAN or SSID:

```plaintext
Switch(config)# interface vlan <access VLAN>
Switch(config-if)# ip flow monitor monitor1 input
```

Cisco portfolio information on supporting Flexible NetFlow

Cisco Routers and Switchers NetFlow support matrix shown below. Most of the Cisco routers, switches and other network devices support NetFlow. (Reference: Cisco NetFlow white paper)

Table 5. Cisco device NetFlow support matrix

<table>
<thead>
<tr>
<th>Platform</th>
<th>NetFlow Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3K-X</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Catalyst 3850/3650</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Catalyst 4500E</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Catalyst 6500E</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Catalyst 6800</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Wireless Controller 5760</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Wireless Controllers 5520, 8510, 8540</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Cisco ISR G2</td>
<td>FNF (v9) / TNF</td>
</tr>
<tr>
<td>Cisco ISR 4000</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Cisco ASR1000</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Cisco CSR 1000v</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>ASA5500, 5550-X</td>
<td>NSEL (v9)</td>
</tr>
<tr>
<td>Nexus 7000 (M Series I/O modules)</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Cisco NetFlow Generation Appliance</td>
<td>FNF (v9)</td>
</tr>
<tr>
<td>Cisco UCS VIC</td>
<td>FNF (v9)</td>
</tr>
</tbody>
</table>
TNF – Traditional NetFlow: used a fixed seven-tuple of IP information to identify a flow most of the time.
FNF – Flexible NetFlow: template based where the user can define the flow
NSEL – Network Security Event Logging: Event based NetFlow. Supported only on Cisco ASA

Can Netflow based Analytics replace Next-Gen IPS solution?
No, both NetFlow based analysis and signature based perimeter IPS solution complement each other very well. The former offers broader analysis based on headers, while the later is deployed in specific locations, goes deeper and looks in to file level. The following table compares the two solutions:

Table 6. NetFlow Analysis and Next-Gen IPS comparison

<table>
<thead>
<tr>
<th>Specifics</th>
<th>NetFlow Analysis</th>
<th>Next-Gen IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection of Threats</td>
<td>Flow analysis</td>
<td>File analysis</td>
</tr>
<tr>
<td>Positioning</td>
<td>Collector generally placed in a central location. Exporter send flows via UDP</td>
<td>Inline to the protected zone</td>
</tr>
<tr>
<td>Inspection</td>
<td>Broader (based on headers)</td>
<td>Deeper (File level analysis)</td>
</tr>
<tr>
<td>Privacy</td>
<td>Looks only header level. User data not looked in to</td>
<td>Inspects files and applications</td>
</tr>
<tr>
<td>Storage</td>
<td>Flow information are lighter and can be stored for months to years for forensics</td>
<td>Storing every packet or file is not feasible, Only logs can be stored for long</td>
</tr>
<tr>
<td>Host based analysis</td>
<td>Based on flows, no client required</td>
<td>Can be client based, like Fire-AMP</td>
</tr>
</tbody>
</table>

NetFlow assists in network behavior analysis (NBA), which is useful in security anomaly detection, but it doesn’t prevent the attack from taking place, rather it triggers an alarm for the security incident. The signature based IPS solution is capable of preventing a potential security attack from occurring by shunning the flow that triggered the signature. However it doesn’t analyze flows to identify deviations from baseline network activity when it occurs.

A comprehensive cyber threat defense solution will include both types of analytics. Correlation of all the possible alerts helps narrow down threats quickly and defend in real-time. To read more about Cisco Cyber Threat Defense solution 2.0, go to [http://bit.ly/cisco-ctd-2-0](http://bit.ly/cisco-ctd-2-0)

Summary

What is NetFlow?
NetFlow is an important tool for network security analysis and cyber forensics. It provides real-time network monitoring and identification and classification of both known as well as unknown day zero denial of service attacks, viruses and worms. NetFlow data provides useful insight into any changes in network behavior, which could help indicate anomalies in data flow. The flow data is also a valuable forensic tool to understand and replay the history of security incidents. NetFlow data can be also used to meet security compliance requirements for various industry standards such as PCI, HIPAA, SOX, etc.

Why un-sampled / Full NetFlow:
Unlike sFlow that is a sampling technology un-sampled NetFlow captures all IP flow information flowing through an interface and reports the entire traffic data without missing any transaction. While flow sampling is a valid method for network management use cases sampling is bad for security use cases because it has the potential to omit certain flows that could be potential network breach that should have been captured in the first place. Full NetFlow provides un-sampled accounting of all network activity on an IP flow enabled interface and is useful in event correlation and data analytics for network security purposes.
Flexible Netflow is better for security.

Traditional NetFlow tracks seven fields in an IP flow namely IP addresses, ports, protocol number, TCP Flags and interface. Flexible NetFlow extends this and allows the user to literally select almost any field from the IP packet, all types of TCP flags and other information too for example VLAN tags. For security purposes this is even better as it provides the user the ability to capture and customize specific bits of information fields from the IP flows which could be important from forensic analysis – for example FnF can be used to perform deep packet analysis on IP flows and extract only those bits of information which is critical for security threat analysis.

Lancope and Flexible NetFlow deliver optimal solution to mitigate cyber threats

Cyber threat is dynamic in nature and hackers are becoming increasingly sophisticated in their attacks. The IT departments of organizations needs to be vigilant and proactive to quickly identify all kinds of cyber-attacks and nuke them before those attacks can manifest themselves. Implementing un-sampled NetFlow in conjunction with Lancope's StealthWatch System acting as a security focused NetFlow collector can help IT department to quickly detect and mitigate cyber threats. Lancope's StealthWatch System protects against advanced threats by delivering in-depth visibility into the network without relying on signature updates to detect attacks by leveraging flow data with sophisticated, behavioral analysis. The joint solution provides enhanced NBA capabilities that could be used to trigger alarms when a network anomaly is detected to proactively identify potential security incidents for further investigation.

For more details visit: http://cisco.com/go/enterprise