BUYER’S GUIDE
Not All NetFlow™ Systems Are Created Equal
Overview

NetFlow™ is a valuable network protocol that provides detailed IP traffic information available from many routers and switches. Utilizing NetFlow provides in-depth visibility into network behaviors, which can greatly improve the security posture and performance of an enterprise network. There are many systems available that utilize NetFlow data, all varying in complexity and in how well they are able to provide actionable insight. This document provides key criteria for evaluating systems that collect and analyze NetFlow to determine their efficacy for various network environments.

Flow Analytics Versus Flow Collection

The first step in leveraging NetFlow is to deploy a platform that can collect and store flow data. There are many systems on the market that perform flow collection, which essentially just stores flow records and provides simple reports on cumulative data. Any investigation or analysis of these records must be done manually, and is highly labor intensive since large networks can produce substantial amounts of NetFlow records. Converting NetFlow records into relevant, actionable data requires flow analytics. Flow analytic systems such as Lancope’s StealthWatch analyze the flow data and provide relevant and actionable information to network operations and security teams. Here are some key features of systems that perform flow analytics:

► Flow Deduplication: A device communicating with a server may traverse several routers and switches that produce NetFlow. A NetFlow record for this session will be exported by each device that the data traverses. Flow deduplication will take these redundant records and consolidate them into one cumulative record while maintaining the data for each hop. Deduplication filters the amount of flow records that need to be analyzed when investigating network traffic, thus reducing the time and effort required for analysis by network and security staff. This feature not only improves the analysis of flow data, but also increases the amount of records that can be stored on the system.

► Flow Stitching: NetFlow records are unidirectional. Flow stitching is the process of taking the unidirectional flows for the traffic sent between two devices and marrying them into one bi-directional record. A system performing flow stitching must be able to do so for both synchronously and asynchronously routed traffic. Flow stitching will provide the complete conversation between two devices in one record, which is critical when performing any type of network or security analysis.

► Flow State: NetFlow records allow you to see the state of a session, whether it is active, inactive, completed or ongoing. Flow state information is important when analyzing flow data since it provides context around the session between two devices. Systems that do not record flow state will only provide cumulative counters between two devices, which limits the ability to perform real-time investigation and troubleshooting.

► NetFlow Data Retention: Maintaining flow records for an extended period of time is very useful for forensic investigation, trending and troubleshooting. The ability to store all network flow conversations is a key element of any flow analytics solution. Due to scalability and storage issues, many systems retain only what are considered “interesting” flows, and provide only cumulative counters for historical analysis. Any enterprise that has regulatory requirements for data retention and investigation will require storage of the flow information for a minimum of 30 days with 90+ days being a common requirement. Many StealthWatch deployments retain flows for numerous months, some in excess of a year within a single platform.

► Intelligent Flow Analysis: Analyzing NetFlow data and performing tasks such as baselining and behavioral analysis is very useful for both security and network operations. The ability for a system to analyze thousands of concurrent flow records and provide the most significant events provides organizations with better security and saves significant time versus manually analyzing and trending data. StealthWatch has been developing patented technology that intelligently analyzes flow data and identifies network anomalies for more than 10 years.
**Actionable Flow Insight:** The ability for a system to analyze flow data and provide alarms identifying events that require analysis is a key component to any flow analytics system. Highlighting these events removes much of the manual analysis that would be required by simple flow collection systems. StealthWatch has a patented Concern Index™ that identifies hosts that have had a significant change in behavior or that are violating policy, and provides a prioritized list of hosts that require investigation. The Concern Index and alarms in StealthWatch also identify the root cause of the change in behavior such as data loss, worm infection or rogue applications/devices.

**Usability of Flow-Based Technologies**

The last thing a network or security engineer needs is another data source that requires time-consuming, manual investigation in order to find interesting events. StealthWatch makes NetFlow analysis easy, so that even a Tier 1 help desk analyst can make sense of it. Here are some key aspects of usability to consider when evaluating flow-based technologies:

- **Identity Correlation:** Investigations with StealthWatch either begin or end with the User ID and MAC address of the host in question. IP address information contained in ordinary NetFlow collectors is not enough. To speed up troubleshooting, StealthWatch ties User IDs to all authenticated hosts on the network, eliminating the need for the analyst to manually query the domain controller for that information.

- **Flow Mapping and Visualization:** NetFlow in the hands of most collectors consists of large tables with thousands of rows of data that do not provide meaningful information. StealthWatch presents flow data visually, allowing for patterns and trends to be easily spotted and enabling Tier 1 analysts to conduct simple investigations without combing through manual spreadsheets of log data. Visual representations of how traffic is flowing through the network increases situational awareness and greatly simplifies root cause investigations.

- **Flow Reporting by IP, Username, Application, Virtual Server and Interface:** NetFlow starts as a single host communicating with a server. Value begins to be derived when higher level summary reports on different types of “objects” can be presented by aggregating statistics from a particular router/switch interface, virtual server or Layer 7 application. These reports are available on-demand within StealthWatch and require no special report configuration.
Host Grouping Using Zone or Logical Format to Match Any Network: Domain-level and host-level statistics are important, but the ability to report on group level (by department/function or location) really separates StealthWatch from other flow-based technologies. The ability to categorize all email servers into a single bucket allows a company to know exactly how much traffic is associated with email while still being able to focus on a single remote office that may contain its own email server. StealthWatch is flexible enough to match the logical breakdown of any network. For example, groups of related IP addresses can be automatically imported into StealthWatch, alleviating a lot of manual set-up and reducing start-up time.

Workflow for Investigation: Getting to the root cause of an incident is the top priority. NetFlow can reduce the time it takes to remediate incidents, but only if there are logical workflows built into the product. With StealthWatch, the root cause of security, network and application response issues is always three or fewer mouse clicks away, greatly reducing mean time to know (MTTK). Reducing MTTK is the key to increasing the productivity of existing staff, enabling them to concentrate on strategic projects versus perpetually troubleshooting issues.

StealthWatch features an intuitive dashboard that enables simple visualization of exactly what is going on inside a network.
Purpose-Built Platform

Most companies have experienced technologies that try to collect, analyze and present a large volume of data on a single appliance. Unlike other technologies, StealthWatch was developed on a purpose-built platform that separates these processes into multiple tiers. From the StealthWatch FlowReplicator™ that collects and distributes the raw flow data, to the StealthWatch FlowCollector™ whose sole purpose is to analyze the data, to the StealthWatch Management Console that presents the data to the end user, speed and scalability are paramount to Lancope.

► **Scale:** There are two variables that pertain to the scalability of a NetFlow system. These are number of NetFlow exporting devices (routers/switches) and flows per second. The latter variable is especially important, and not just under normal conditions. When there is an incident, flow volume can spike many times above the average level. With that in mind, organizations must ensure that their NetFlow engine can handle the flow volume under adverse network conditions. StealthWatch can handle 25,000 NetFlow exporting devices and 1.5 million flows per second under normal operations (and about 3.5 million flows per second for short duration). Organizations should be aware of any vendor quoting flows per minute, as that is not how routers/switches calculate their flow volume. This method is used to artificially inflate capacity by showing a much bigger number than if scalability was rendered in flows per second.

► **Data Retention and Forensics:** It is important that a NetFlow engine be able to record months of flow data without having to archive anything to a secondary storage device. This is especially true for auditing and compliance purposes, where Lancope is seeing a growing trend of at least six months of flow data being required. An organization will never know when they might be asked to produce flow data from four months ago on a Saturday at 4:00 a.m. For even the largest organization, almost any length of storage can be achieved with a single StealthWatch Management Console. This is important for a forensics investigation during which the data must be present and accessed on a timely basis without having to look for it on secondary storage devices.

StealthWatch harnesses the full power of flow data to provide comprehensive visibility across the entire network.
**System Performance:** With potentially billions of flow records on a single system, flow information must be rendered in a timely manner. NetFlow is meant to be used for near real-time operations, so that any collector that requires the operator to go get a cup of coffee after pressing ‘go’ on a query should automatically be discounted. StealthWatch has a very scalable, column-oriented database that allows it to go through billions of flow records and return answers quickly. Many “top x” reports are pre-run so that they return almost instantaneously. On any system, try running a query over the last week, looking for outbound flows over 1 MB in size using only the http application and see how long the query takes to come back.

**Different Network Vendors, Different Flow Types**

Today most networking vendors include support for some type of flow technology, such as NetFlow (Cisco), J-Flow/cflow (Juniper), sFlow (HP, Foundry, Extreme, Alcatel) and IPFIX (Nortel), which can be used for network performance or security monitoring of today’s complex networks. When looking for a flow analytics solution, choose a solution that will support multiple vendors’ flow technologies to provide flexibility and future-proof your network performance and security monitoring investment.

**Support for Latest Flow Technologies**

NetFlow has advanced over the past few years with new technologies such as Flexible NetFlow and IPFIX. The latest flow technologies are based on NetFlow v9, which includes additional information fields outside of the standard seven, including but not limited to vendor-specific ID, application awareness (NBAR), QoS and RTT. Organizations should be asking about these new technologies and fields when evaluating flow-based monitoring solutions.

**Application Awareness**

Today’s Internet-bound traffic is no longer simple HTTP traffic. In some respects, port 80 has become the new TCP. More applications are using (or provide the end user the ability to change the communication port to) a commonly used port such as HTTP port 80. Having the ability to identify the application tunneling over common ports is important for capacity planning and for identifying data loss and malicious traffic.
Visibility into the Virtual Network

As companies look for ways to consolidate resources and reduce costs, virtualization of server resources has become very popular. Administrators are being challenged to monitor not only traffic entering or leaving the ESX host, but also the communications between virtual machines. The following considerations should be made when looking at a NetFlow solution to monitor traffic and security within the VM environment:

► How is the virtual sensor implemented? Lancope’s virtual sensor is installed as a VM instance and is capable of monitoring the virtual switch within the ESX host. This allows StealthWatch to see all communications between VM instances. It is a lightweight resource that does not use up excessive virtual server resources since the analysis of the generated NetFlow data takes place on the purpose-built NetFlow collector, not within the ESX host.

► What are the capabilities of the virtual sensor? Lancope’s virtual sensor not only monitors traffic between VM instances, but it can also monitor for a VMotion event and provide an alert when one takes place, so that administrators are notified about unauthorized moves.

Third-Party Integration

Security operations teams rely on many different tools to secure today’s networks. These tools range from SIEM and IDS/IPS to vulnerability management and firewalls, as well as various others. StealthWatch is capable of integrating with most third-party solutions used by today’s IT security teams, easing network management and enabling organizations to deploy defense-in-depth security strategies.

Harnessing the Power of NetFlow

NetFlow provides an extremely valuable and cost-effective means of improving network performance and security efforts. However, not all NetFlow systems are created equal. It is therefore very important to carefully consider the facets discussed above to select the NetFlow collection and analysis system that will make the biggest, most positive impact on your specific infrastructure.

To learn more or request a demo, contact sales@lancope.com.
Checklist for Flow-Based Monitoring Solutions

Not all NetFlow solutions are created equal – they vary greatly in capabilities and usability. Effective, flow-based monitoring tools should include the following:

<table>
<thead>
<tr>
<th>Lancope</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Flow Deduplication</td>
</tr>
<tr>
<td>✔️</td>
<td>Flow Stitching</td>
</tr>
<tr>
<td>✔️</td>
<td>Flow State Information</td>
</tr>
<tr>
<td>✔️</td>
<td>Long-Term Flow Data Retention</td>
</tr>
<tr>
<td>✔️</td>
<td>Intelligent Flow Analysis</td>
</tr>
<tr>
<td>✔️</td>
<td>Actionable Flow Insight</td>
</tr>
<tr>
<td>✔️</td>
<td>Identity Correlation</td>
</tr>
<tr>
<td>✔️</td>
<td>Flow Mapping and Visualization</td>
</tr>
<tr>
<td>✔️</td>
<td>Flow Reporting by IP, Username, Application, Virtual Server and Interface</td>
</tr>
<tr>
<td>✔️</td>
<td>Host Grouping Using Zone or Logical Format to Match Any Network</td>
</tr>
<tr>
<td>✔️</td>
<td>Workflow for Investigation</td>
</tr>
<tr>
<td>✔️</td>
<td>Scalability</td>
</tr>
<tr>
<td>✔️</td>
<td>Data Retention for Forensics</td>
</tr>
<tr>
<td>✔️</td>
<td>System Performance</td>
</tr>
<tr>
<td>✔️</td>
<td>Support for Various Flow Types</td>
</tr>
<tr>
<td>✔️</td>
<td>Support for Latest Flow Technologies</td>
</tr>
<tr>
<td>✔️</td>
<td>Application Awareness</td>
</tr>
<tr>
<td>✔️</td>
<td>Virtual Network Visibility</td>
</tr>
<tr>
<td>✔️</td>
<td>Third-Party Integration</td>
</tr>
</tbody>
</table>

About Lancope

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales
+1.770.225.6500
888.419.1462

International Sales
+44 (0)560 344 8075

Website: www.lancope.com
E-mail: sales@lancope.com

©2011 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners.

BGV605162011