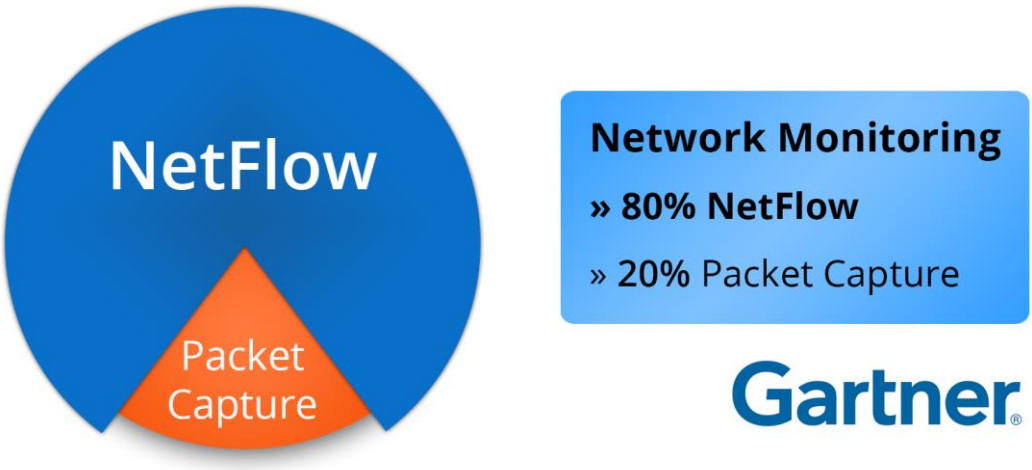
Advanced solution for network traffic visibility

Document purpose

Providing a stable computer network and control over network applications is a critical task for organisations where nearly all communication uses a shared network infrastructure. Network administrators face a dynamic environment with a growing number of applications and an increasing amount of transferred data, mobile end devices that are often employee-owned (BYOD), virtualisations, distributed infrastructure and cloud services. These new concepts place more demands on the stability and administration of a computer network and its ability to perform the organisation's key processes as well as routine operations.

Network administration departments clearly need new and powerful tools to do their job effectively. Such tools are designed to provide the necessary visibility into communication at both the device and network level, and control over network applications. This allows them to reduce the time between the occurrence and resolution of a network problem and to proactively avoid network and application problems.



This document describes:

- The key challenges in network administration and network traffic analysis
- The architecture of our solution for advanced network traffic analysis
- The benefits of modern flow monitoring technology
- The Cisco and Flowmon Networks combined solution

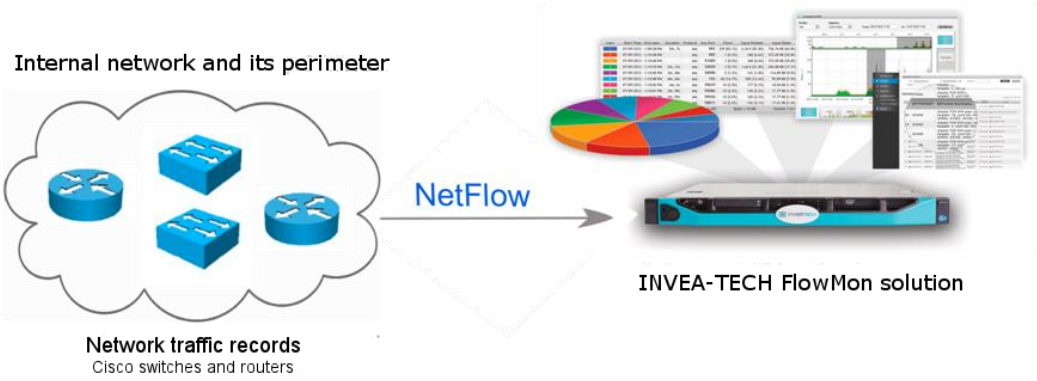
Challenge

Corporate and WAN networks' data rates of up to tens of gigabits allow organisations and staff to transfer vast amounts of data both within their internal network and when communicating on the Internet. Many services are provided through the cloud or a distributed infrastructure. Mobile devices are often used as an access point and organisations deploy new systems, many of which are critical to their operations. As a result of the BYOD trend, devices beyond the control of a network administrator are connected to the network, bringing unauthorised applications into it or consuming a large portion of network capacity.
A network administration department needs appropriate tools to maintain the necessary control over the network under such circumstances. The widely used SNMP monitoring technology is insufficient in terms of network visibility while traffic capture technology is not usable for long-term network-wide monitoring. Network administrators need detailed information about how much data is transferred in the network as well as about which stations generate that data, where it is sent, what type of traffic or application it is and whether such transmissions pose a threat to network stability and security. A similar view is required at the level of applications that are used by the organisation or occur in its network. Such information, both real-time and historical, must be available for the entire network, i.e. for each single device connected to the network. Given the amount of the data captured, some automatic processing and detection of network incidents will also be necessary.

Solution architecture

Our solution for advanced network traffic analysis combines the following features for complete network visibility and effective data processing:

- Active Cisco components provide visibility into network traffic and are capable of generating complete (unsampled) NetFlow records of network communication (they support Cisco switches and routers). Using the Cisco AVC technology and the Cisco NBAR standard, the same components provide application visibility and monitor performance indicators.
- The Flowmon collector by Flowmon Networks stores, processes, analyses and reports network traffic information. The collector supports the Cisco NetFlow v5, v9, NBAR2, AVC standards as well as the IPFIX and sFlow general protocols.



As the Flowmon solution can process NetFlow and NBAR2 or AVC information from Cisco switches and routers, Cisco components in the client's network that support the export of such data may be used. This deployment reduces purchase costs and adds value to the client's investment in Cisco infrastructure.

Solution benefits

Our solution for advanced network traffic analysis aims to provide a detailed insight into an internal network and to detect operational and security incidents in the network. The key benefits of the solution are:

- Detailed records of the organisation's internal network operations
- Easier and faster network troubleshooting
- Control over network application traffic (application awareness)
- Detailed monitoring of data network performance
- Detection of selected operational and security events at the network level
- Early detection of network problems and incident prevention
- Periodical network status reporting, network capacity planning
- More efficient and less demanding network administration
- Better network availability and stability
- Possible use of an existing Cisco infrastructure in the network

In addition to Cisco, NetFlow data analysis as a key technology for enhanced network availability and stability is recommended also by the Gartner analytical group.

Solution components

Generating traffic information across the network

The new functionality of Cisco Catalyst switches and routers allows for integrated monitoring of network traffic – from user workstations to servers and mobile devices. The Cisco Catalyst 3560-X, 3750-X, 3850, 4500, 6500, Cisco Nexus switches and all Cisco routers provide native NetFlow data export without compromising device performance.

NetFlow data aggregation, logging and analysis

NetFlow data is analysed using the Flowmon solution by Flowmon Networks. With real-time data processing, Flowmon enables immediate response to network disruptions. Flowmon also stores long-term network traffic history, delivering essential information in order to analyse traffic even over several months.

Primary component of the Flowmon solution:

- Flowmon collector – for the aggregation and storage of NetFlow data from an unlimited number of sources. The collector provides advanced tools to report and analyse network and application traffic.

Flowmon extension components include:

- Flowmon probes – special devices used to generate NetFlow data, identify applications, monitor performance and analyse VoIP traffic in an environment where it is impossible to generate such data using an existing Cisco infrastructure.

The Flowmon solution is available as a physical or virtual appliance.

Benefits of our solution for advanced network traffic analysis

The unique combination of Cisco products able to generate NetFlow records and the Flowmon solution to process such data cuts the time needed to troubleshoot network problems, improves network stability, provides the necessary control over network applications and reduces network administration costs. Also, the costs of implementing and running this solution are minimal for customers that use Cisco products in their infrastructure.

For more information

For more information, please contact your Cisco or Flowmon Networks partner.

Cisco Systems (Czech Republic) s.r.o.
V Celnici 10
117 21 Prague 1
Czech Republic
www.cisco.com

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno
Czech Republic
www.flowmon.com