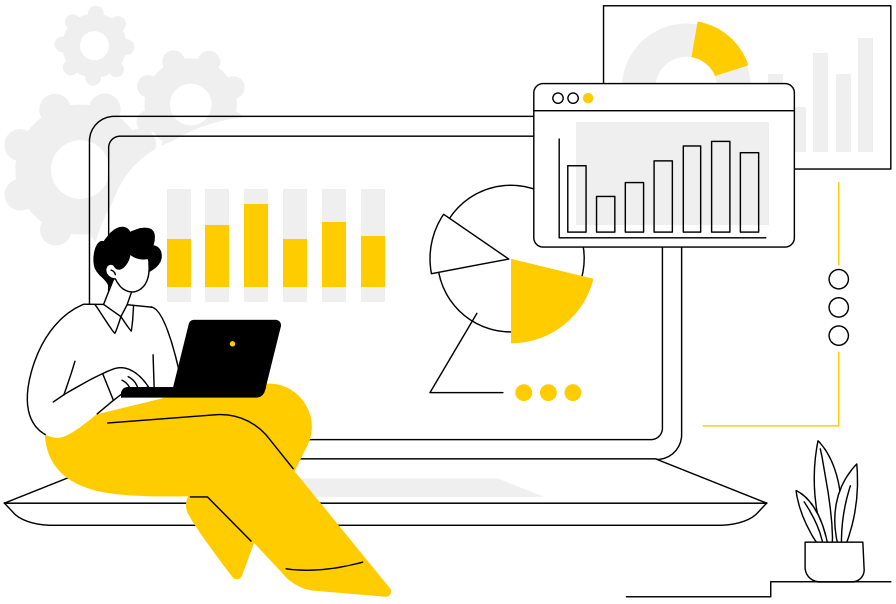
ManageEngine
NetFlow Analyzer

Enterprise network traffic management



Summary

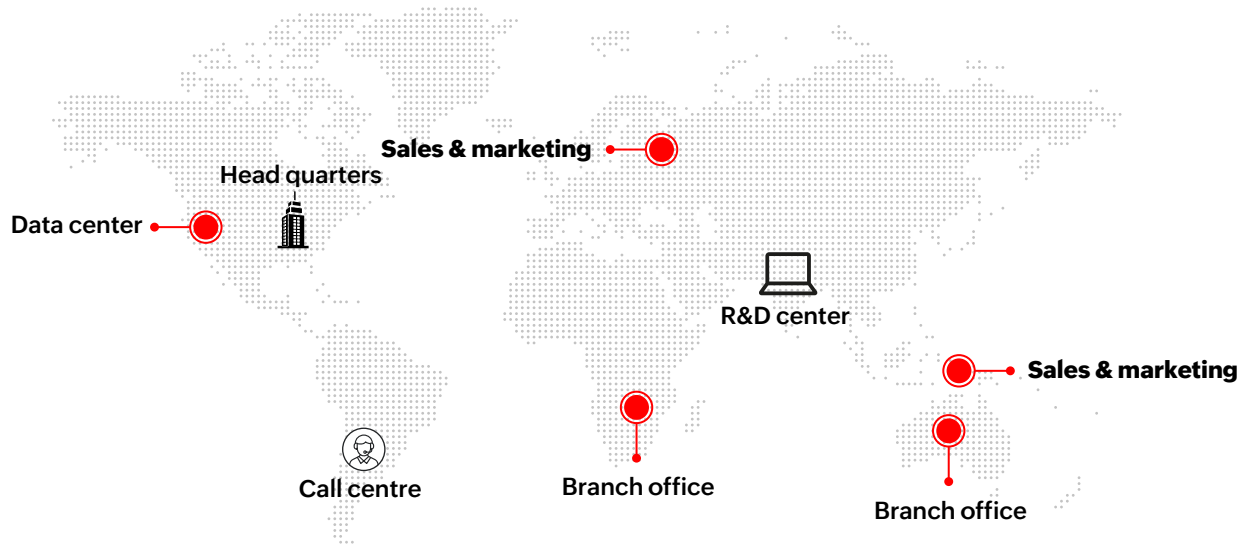
This paper highlights the importance of having an enterprise-wide network traffic analysis tool in today's global enterprise. By harnessing the data contained in flow exports (NetFlow, sFlow, CFlow, J-Flow, NetStream, and IPFIX) from routers and switches, you can get deep insights in to your network traffic, including the who, what, and why of bandwidth usage.

This information is vital for IT heads to make the right strategic decisions that can benefit the whole organization. This paper discusses the advantages of deploying a flow-based software solution that uses distributed collection. Unlike the hardware, which uses probe-based monitoring, a flow-based software solution requires less investment, is easy to install, and delivers value in a matter of hours.

Table of contents

1. The end of business as we know it

In today's fast-changing business landscape, computer networks play a vital role. No longer is business confined to the four walls of the enterprise. Large enterprises today need to pursue strategies like offshoring, outsourcing, smart-sourcing, etc. to be competitive. Implementing these strategies globalizes the nature of work, meaning work gets done across geographies and time zones. Welcome to the distributed enterprise!



Today's enterprises are pursuing some of these strategies:

- It is common to see enterprises base their headquarters out of the UK; the suppliers of raw materials (supply chain) out of China, Brazil, and Norway; the knowledge workforce out of India; and its sales and marketing staff spread across the globe. It's also common to see much of its sales happen the e-commerce way.
- To avoid legal hassles and comply with the growing number of data integrity and security mandates (such as HIPAA, SOX, and the like), enterprises today prefer to have their entire database on all aspects of their business in a secure, central data center, mostly based in the US.

- To overcome the cost associated with deploying skilled network administrators at various distributed office locations and also to overcome the challenge of skilled finding personnel, enterprises prefer centralized monitoring of their global networks.
- Every enterprise that wants to cut costs and remain competitive is doing away with the costs associated with acquiring proprietary software and applications. The emerging trend is enterprises moving towards the Software-as-a-Service (SaaS) model. This includes web-based applications like Salesforce.com for sales force automation, Zoho for enterprise productivity, etc.
- Facilitating access and communication between the various constituents of the distributed network and ensuring access to the datacenter/SaaS application from the remote offices becomes crucial. Also, to monitor the whole network from a centralized location, having a unified view of the entire network becomes indispensable.

In today's fast-changing business landscape, computer networks play a vital role. No longer is business confined to the four walls of the enterprise. Large enterprises today need to pursue strategies like offshoring, outsourcing, smart-sourcing, etc. to be competitive. Implementing these strategies globalizes the nature of work, meaning work gets done across geographies and time zones. Welcome to the distributed enterprise!

2. Enterprise bandwidth management: A strategic requirement

With network domain changes sweeping enterprises these days, it falls on the network administrator to ensure a high level of WAN availability all the time. As an enterprise becomes a global presence, managing the health and performance of the entire network, including remote and branch offices, becomes a challenge.

Any degradation in network performance anywhere in the network could lead to significant productivity loss and employee frustration. It gets all the more important to be sure that no unwanted traffic, network abuse, or network attack is happening at any point in time.

The main challenges in such a scenario include:

1. Ensuring strong network connectivity and constant bandwidth availability. Bandwidth should not be a limiting factor to a business' success.

2. Ensuring optimal bandwidth for critical applications. Ensure revenue-generating applications take precedence over trivial applications. Prioritize critical applications like access to SAP HRMS, Oracle Financials, Zoho CRM, and Salesforce.com, or access to the company's IBM mainframe over trivial things like streaming videos, downloading music, etc.

3. Quickly troubleshooting any network incidents, pinning down the root cause of problems to fix them fast.

4. Accurately planning capacity, as the costs involved are huge when it comes to large enterprises.

5

Keeping tabs on the globally spanning network.

- Be in the know: Is your enterprise network bandwidth being used correctly or abused?
- The lack of availability of qualified network administrators can be overcome by delivering centralized monitoring to the network manager.

6

Ensuring the quality of the service delivered by the ISP is in line with the terms of the agreement.

The only way to address these problems is by having a powerful enterprise-wide bandwidth monitoring and traffic analysis tool. With knowledge of the traffic patterns in similar departments across offices and geographies and information on what's consuming bandwidth, a network admin or CIO can enforce the appropriate policies to restrict undesired bandwidth usage—like downloading music files or watching YouTube videos during business hours.

This unified, collective view of bandwidth consumption also helps with making accurate strategic decisions on capacity planning (ordering more bandwidth). Also, having access to historic data of traffic usage pattern helps to benchmark current usage levels.

3. Typical approaches to bandwidth monitoring

There are various types of bandwidth monitoring solutions to choose from. In general, they can be classified based on the underlying technology (data acquisition technique).

Based on data acquisition

Bandwidth monitoring solutions typically adopt one of these techniques: SNMP query, test access ports (TAPs), Switch Port Analyzer (SPAN) ports, packet sniffing, or analyzing flow exports like NetFlow, sFlow, Cflow, J-Flow, NetStream, and IPFIX.

SNMP uses SNMP queries on SNMP agents running in the network device to get information on the bandwidth usage in the network. SNMP query gives a consolidated or bulk traffic figure. So, this needs to be complemented with in-depth network traffic analysis that answers questions like who's using what bandwidth and when. However, since SNMP uses pull technology, it may end up consuming a considerable amount of your enterprise's bandwidth.

SPAN ports are designated on switches to mirror traffic received on other ports. TAPs are traffic replicators placed in between two routers, firewalls, or enterprise switches that sends a copy of all the network traffic flowing through them. SPAN and TAP ports can be used to forward network traffic to software applications or hardware probes for traffic analysis to obtain network traffic information. The downside is the cost involved in procurement, deployment, and management of these types of ports.

A packet sniffer intercepts and collects local traffic by capturing the packets from the network that the sniffer is attached to. A sniffer is used in network troubleshooting,

network intrusion detection, and network usage monitoring by displaying actual traffic insights by IP address and protocol. The downside is the heavy load on the monitoring system.

Flow-based technology harnesses the information contained in flow exports like NetFlow, sFlow, Cflow, J-Flow, NetStream, and IPFIX and presents an in depth view of the traffic flow. They offer a scalable and a low cost approach to have deep insight into the network traffic based on layer 3 and layer 4 packet information. With this information, you'll know who's using what bandwidth and when.

Using the data extracted from the flows, you'll know:

- Who the top talkers on the network are.
- When traffic peaks and why.
- How long bandwidth use spiked and why.
- The source and destination involved in a conversation.

This approach provides the information necessary to make capacity planning decisions, to detect any form of network abuse in monitoring QoS, and, to a certain extent, to identify security attacks.

The below table lists the flow type for the following vendors.

Type of flow	Supporting vendor devices
NetFlow	Cisco, Enterasys, Extreme Networks, Foundry Networks, 3com, and Riverbed
sFlow	Alcatel, Extreme Networks, Foundry Networks, Hitachi, NEC, Alaxala

	Networks, Allied Telesis, Hewlett Packard, Comtec Systems, and Force10 Networks
Cflow andJ-Flow	Juniper
NetStream	Hauwei and H3C
IPFIX	Nortel

Table 1: Various flows supported by vendors: ***Learn more***

Let's look at an example of a software solution that is based on harnessing the data contained in flows to monitor an enterprise's network bandwidth.

4. A flow-based software solution

When a global enterprise decides to use a flow-based software solution for monitoring its distributed global enterprise, the setup looks like the figure below. The software has to be deployed in each of the remote locations and the data gathered from the location is visible to the network admin at that level or location only.

When a global enterprise decides to use a flow-based software solution for monitoring its distributed global enterprise, the setup looks like the figure below. The software has to be deployed in each of the remote locations and the data gathered from the location is visible to the network admin at that level or location only.

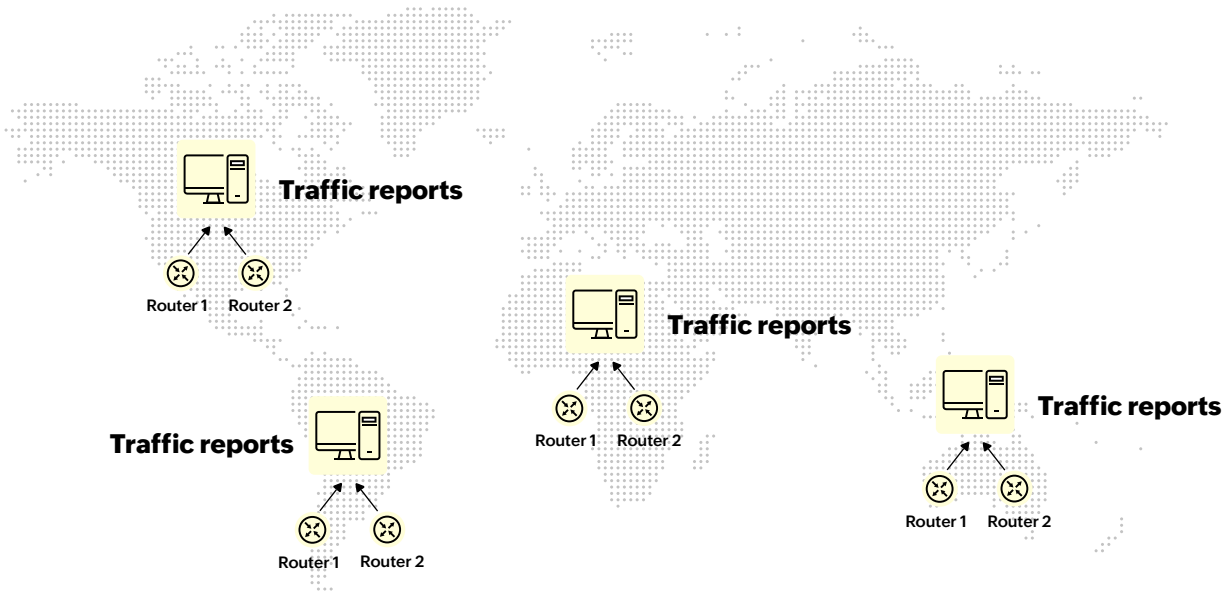


Figure 2: Typical flow-based monitoring

The report on the bandwidth usage in each of the offices is visible only to the network administrator at that office. Here the data is in silos. For a consolidated overall view, the data available with each network admin has to be collated by the chief network administrator or CIO.

Drawback of this solution

- Lack of a unified view:

  A distributed monitoring solution can fix the drawback in the above model. By collating data from all the distributed locations and presenting it in a unified view, it offers greater control to the chief network administrator or CIO.

5. A flow-based distributed monitoring solution

Case in point: The NetFlow Analyzer Enterprise edition

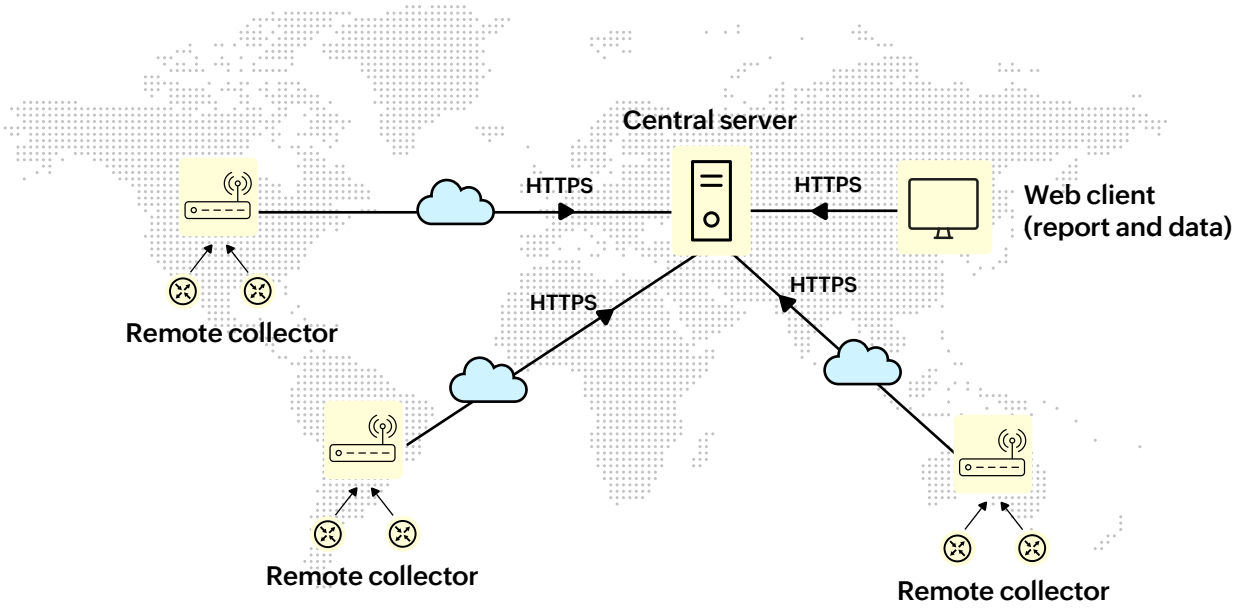
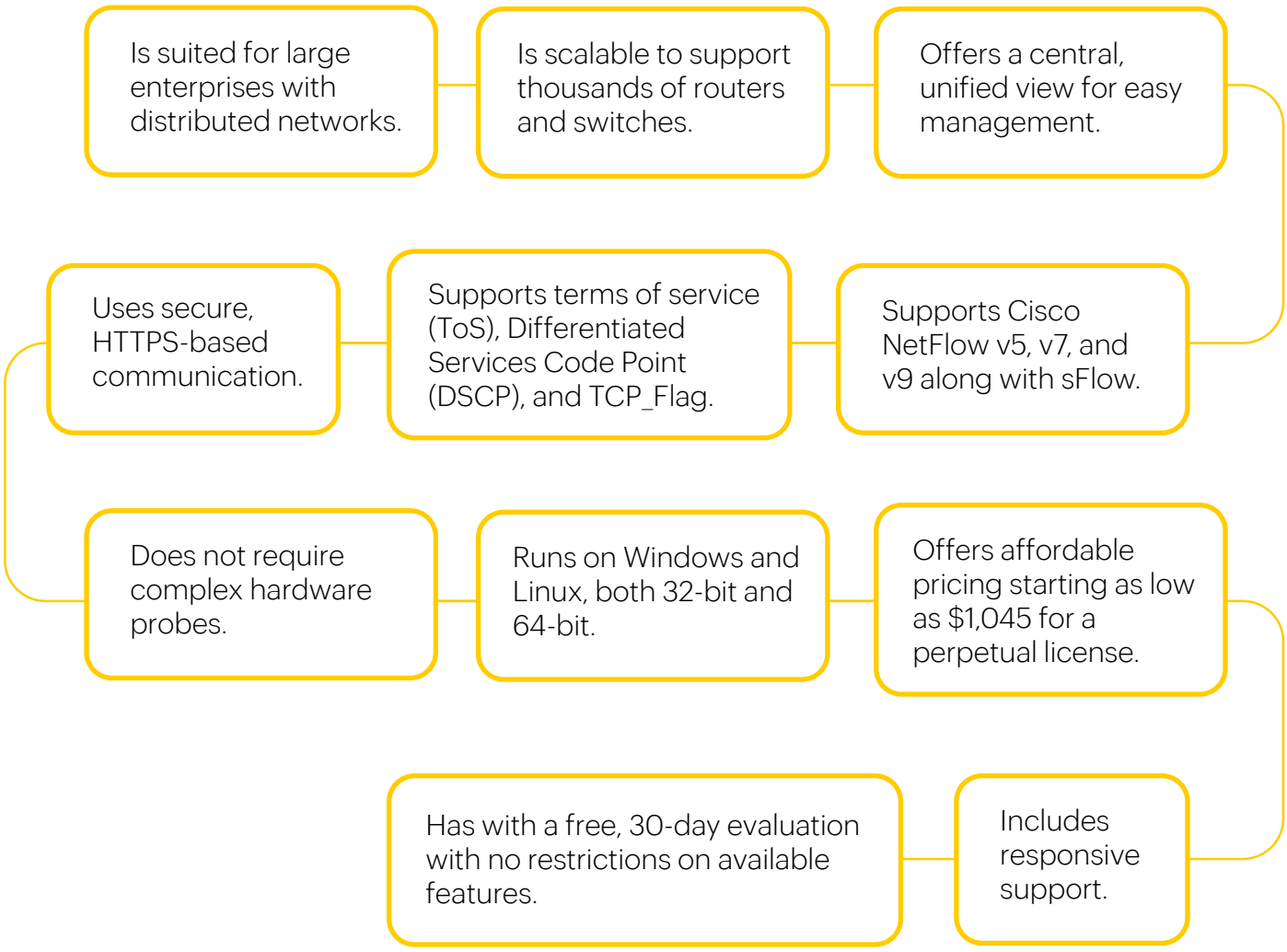


Figure 3: Flow-based monitoring with distributed collection

The NetFlow Analyzer Enterprise edition is a flow-based scalable software solution from ManageEngine that's ideal for large corporations with tens of thousands of interfaces. It uses distributed collectors (shown in the diagram above), which are installed in remote offices. The remote collectors collect the flow information from all the routers in the location, process and compress the data, and send it to the central server through a secure HTTPS link. This way, the resources that are consumed are just a fraction of what would be consumed by other traffic monitoring techniques.

The central server receives the compressed data exported by all the collectors and further analyzes it for reporting. The central server is ideally located at the company's main headquarters. A chief network administrator or CIO can then access the reports generated by the central server through a web client and get a unified view of the entire network.

The NetFlow Analyzer Enterprise edition:



6. Conclusion

Take in to consideration the below key points before choosing your traffic analysis and bandwidth monitoring solution to ensure that your investment delivers the expected value.

9 Key points for the CIO or network manager to consider in choosing the right solution

1. Consider what kind of solution you need: a hardware, probe, packet analyzer-based solution or a purely software-based solution.
2. Consider the cost of the solution. You need to know what the cost of using the software over the next five years will be.

    i. Clarify the cost associated with software upgrades and product support.
    ii. Confirm on the costs associated with having personnel deployed to handle challenges as they arise.

3. See the investment in the product versus the product's ROI.

    i. A product that costs more than the ROI it generates is never the right solution.
    ii. Bandwidth monitoring is a function that is meant to add value to the enterprise's bottom line. It should not end up costing the network department more than it returns in value.

4. Evaluate the kind of support the vendor offers.

    i. The number of responsive staff available makes all difference to you as the customer. Ensure your vendor has a fully staffed and readily available support center.

5. Familiarize yourself with the legacy of the company and product.

   i. Typically, a company that has been in the business for more than a decade and has managed to remain profitable is a good choice to go with.
   ii. A product that has supported thousands of customers across the globe is a testament to strong engineering ability and a rock-solid support.

6. Choose a vendor by predicting future needs.

   i. Do not buy a solution considering today's requirement alone.
   ii. Opt for a company that has a wide range of network-management-allied products. In addition to monitoring your whole enterprise network bandwidth, in the future, you may want to monitor the performance of applications in your network, analyze your firewall logs, etc.
   iii. Visualize the future needs of your network and choose a vendor that can meet those needs.

7. Evaluate at your pace.

   Seek extension of your trial license if you're still not convinced it's the right solution. A company that does not oblige to extending your license or has cumbersome procedures to do so may not be the best bet going forward.

8. A vendor's forums can reveal a lot about it.

   See how active and vibrant the forums are. Forums can show how popular the product is and responsive the product teams are.

9. Finally, don't fall prey to consultants and marketing gimmicks!