Cisco IOS Flexible NetFlow

Customer Need: Application Visibility

In an enterprise, hundreds of applications are accessed by users in different campus locations and remotely from a branch or home. The volume of application usage is usually not known beforehand and increases nonuniformly over time. This nonuniform application usage translates to unpredictable increases in traffic across the network, complicating capacity planning. Unpredictable increase in traffic can also be caused by security breaches such as viruses, denial-of-service attacks, and network-propagated worms. Rather than wait for these incidents to happen before tackling them, administrators must have the ability to see the usage pattern in advance for capacity planning and security incident detection and remediation.

Technology Postcard

Feature Description: Flexible NetFlow

Cisco IOS® Flexible NetFlow is an embedded Cisco IOS Software tool that provides customized visibility into network traffic. It is available on most Cisco® switches, wireless controllers, and routers. Cisco IOS Flexible NetFlow collects data that can be used to detect network anomalies that result from security issues and projects the trend in usage for capacity planning.

Cisco IOS Flexible NetFlow answers the question "how many applications are really running in an enterprise?" It can be customized by an IT administrator to monitor applications in use and to view traffic usage by time of day, source, destination, and user applications. Compliance with regulations such as HIPAA and Sarbanes Oxley can be determined. Based on traffic movement, IT knows who is accessing which resources and can appropriately set policies to restrict access for different segments of users.

Cisco IOS Flexible NetFlow can be managed directly on switches and routers, or the Cisco Prime™ management application can simplify management by providing graphical systemwide visualization of the results.

These two use cases show the benefits of Cisco IOS Flexible NetFlow deployment.

Use Case 1

- **Without Cisco IOS Flexible NetFlow:** IT administrators rely on user feedback to learn that traffic usage has reached the network bandwidth limit and that it is time to upgrade network capacity. Or IT upgrades the capacity across the board on a preset timeline. Both are expensive propositions for capacity planning because either companies don't have the capacity needed in time or they overdeploy capacity that isn't needed.
- **With Cisco IOS Flexible NetFlow:** IT administrators can customize Cisco IOS Flexible NetFlow to monitor **applications of interest**. Or they can monitor the entire network to see how different parts of the network are being utilized by application. Reports from Cisco IOS Flexible NetFlow provide trends in usage that help IT optimize capacity planning and allow for selective upgrades that save the organization a lot of money. End users are happier without confronting a network bandwidth limit.

Use Case 2

- **Without Cisco IOS Flexible NetFlow:** A malicious user starts a denial-of-service attack against a server. IT administrators fail to identify an unexpected spike in traffic in that part of the network. The attack brings down the server and its service, affecting many users. Users open IT trouble tickets, prompting IT to investigate and remediate the problem—too late for already frustrated users.
- **With Cisco IOS Flexible NetFlow:** When the malicious user starts a denial-of-service attack on the server, the traffic in that part of the network starts to increase abnormally. This spike in traffic is captured using Cisco IOS Flexible NetFlow immediately when it starts to increase. IT administrators will be alerted about this anomaly, and they can quickly trace the source of the attack and take action, solving the problem before there are end-user complaints.

NetFlow is an older technology with similar benefits. The following table shows the improvement of Flexible NetFlow over NetFlow.

NetFlow	Flexible NetFlow
Always monitors 7 pieces of information in IP traffic. Security detection is limited to what can be obtained from those 7 pieces of information.	The pieces of information to monitor can be customized. Monitors the complete Layer 2 and IP header and TCP flags for comprehensive visibility and security. Flexible NetFlow can also focus on certain types of applications for targeted monitoring.

Benefits

1. Cost effective capacity planning through customized monitoring of applications, making sure of network availability for critical applications
2. Bandwidth usage tracking by users, locations, and applications without any effect on network performance
3. Real-time detection of anomalous network behavior caused by security breaches
4. Supported by many visualization applications, which gather the results and show them in a variety of user-friendly formats

Supported Catalyst Platforms

- Cisco Catalyst® 6500 Supervisor Engine 2T
- Cisco Catalyst 4500E Supervisor Engine 7E/7LE
- Cisco Catalyst 4500-X
- Cisco Catalyst 3750-X
- Cisco Catalyst 3560-X

For More Information

http://www.cisco.com/go/netflow

C22-722462-00 01/13