Progress® WhatsUp® Gold

Network Traffic Analysis

Analyze and Monitor Bandwidth Consumption and Network Traffic

GET VISIBILITY TO NETWORK TRAFFIC

Monitor and set threshold-based alerts on network traffic and bandwidth usage. Collect and view data for Cisco CBQoS and NBAR..

Network Traffic Analysis is available as an add-on to WhatsUp® Gold's Premium, MSP and Distributed editions and is included in the Total Plus edition.

Our Network Traffic Analysis module delivers detailed and actionable data on network traffic and bandwidth consumption, which helps you establish and enforce bandwidth usage policies, control ISP costs, secure the network, and provide the network capacity required by users, applications, and the business. It not only highlights the overall utilization of the LAN, WAN, and the internet, but also indicates which users, applications, and protocols are consuming bandwidth.

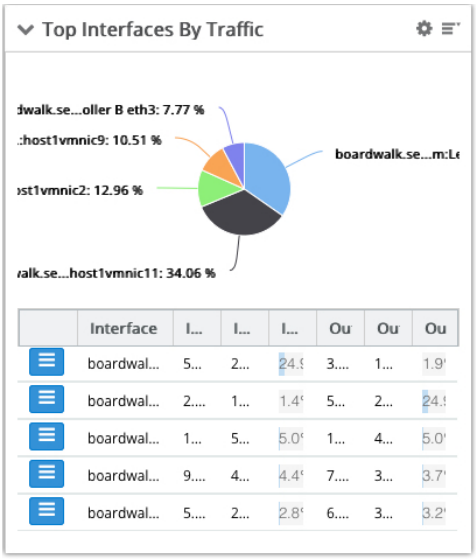
Get Detailed Visibility to Bandwidth Usage Patterns

Monitor your Network Traffic

The Network Traffic Analysis module collects network traffic and bandwidth usage data from any flow-enabled device on the network. It supports Cisco's NetFlow, and NSEL protocols, QUIC, Juniper Network's J-Flow, as well as sFlow and IPFIX. Uniquely, it provides support for Cisco's NetFlow-Lite, eliminating the need to use a 3rd party aggregator to convert flow records from the NetFlow-Lite to Netflow format.

Get detailed visibility to network traffic information on:

- Senders, receivers, and conversations
- Sender and receiver domains
- Sender and receiver countries
- Applications and protocols
- Incoming and outgoing interface traffic
- Incoming and outgoing interface utilization
- Bandwidth usage by host and group



Collect and view data for Cisco CBQoS (Class Based Quality of Service) and NBAR (Network Based Application Recognition).

Receive Alerts about Your Network Traffic

The Network Traffic Analysis module provides threshold-based alerting to help you address network traffic problems before they impact your users, applications, and business. It alerts you when senders or receivers exceed bandwidth thresholds, when interface traffic exceeds utilization thresholds, and when you exceed failed connections and the number of conversation partner thresholds.

The Network Traffic Analysis module allows you to create custom alerts for protocol traffic such as sudden spikes in UDP traffic which may indicate a denial of service (DoS) attack on your network.You can create custom alerts for application traffic. For example, you can get notifications when users are consuming expensive internet bandwidth on non-business applications like YouTube, Spotify, and League of Legends. You can even create custom alerts for host traffic. For instance, receive alerts when

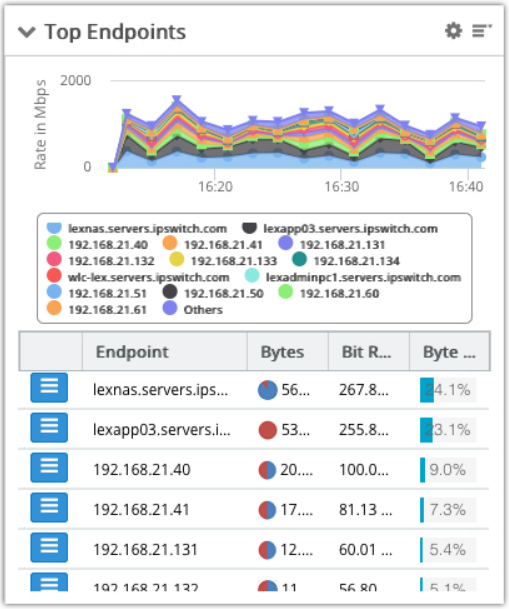
large files containing sensitive data assets are transmitted over the internet. Receive alerts when users exceed bandwidth usage thresholds.

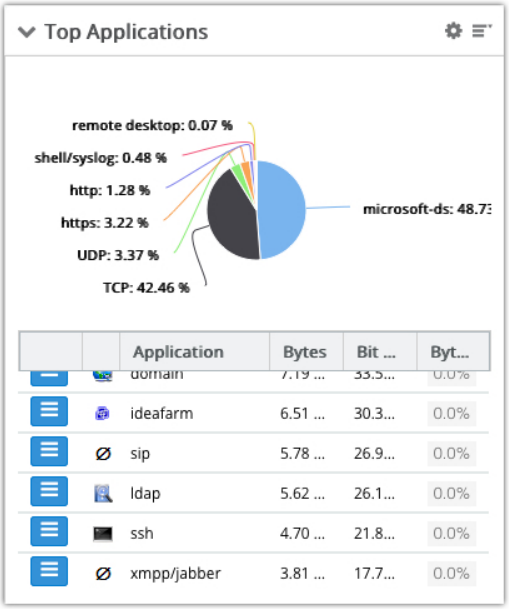
Report on Your Network Traffic

Monthly ISP bandwidth charges are expensive. You don't want to add more bandwidth unless you need it. Our Network Traffic Analysis lets you drill-down to identify the sources and destinations of your internet traffic, the applications consuming internet bandwidth, and the users of those applications. In this way, you can ensure that your business critical web applications are getting the bandwidth they need.

Get dozens of out-of-the-box network traffic reports including:

- Sources
- Interface traffic and bandwidth utilization
- Top senders, receivers, and conversations
- Top sender ASN and top receiver ASN
- Top sender and receiver failed connections
- Top applications and protocols
- Types of devices
- Top NBR application flow details and interface totals
- Class Based Quality of Service (CBQoS)





These powerful dashboards help you identify traffic flow patterns, analyze bandwidth consumption, and isolate and resolve network bottlenecks. The Top Senders, Receivers, and Applications dashboards provides a baseline of what is generating traffic on your network. You can use this to identify potential bottlenecks requiring network redesign and additional capacity, or the need to implement usage policies.

The NBAR Top Applications report displays the network traffic resulting from the top applications as identified using Cisco's NBAR classification engine. The CBQoS reports provide information about the effectiveness of class-based policies.

WhatsUp Gold's Network Traffic Analysis module provides reports that can help you secure your networks by identifying potential Denial of Service (DoS) attacks, evidenced by spikes in UDP traffic, or by highlighting large file transfers from sensitive data assets using Peer-to-Peer Protocols.

For a free trial please visit: www.ipswitch.com/forms/free-trials/whatsup-gold