

## Scrutinizer NetFlow & sFlow Analyzer



My View | Status | Alarms | Vitals | Settings | Help

Top Conversations across 19 flow devices

Source	Prot	Destination	Volume
1 216.115.216.21	https	66.186.184.193	179.5 Mb
2 216.129.125.201	http	66.186.184.195	81.3 Mb
3 66.186.184.204	http	10.1.37.1	70.1 Mb
4 64.233.179.91	http	66.186.184.193	63.1 Mb
5 66.186.184.1	MOS Monitoring	24.63.55.179	47.3 Mb
6 64.63.55.179	MOS Monitoring	66.106.104.1	47.3 Mb
7 205.243.60.42	http	66.186.184.193	46.7 Mb
8 72.47.210.50	http	66.186.184.193	40.9 Mb
9 216.115.216.21	https	10.1.1.63	29.7 Mb
10 66.102.1.99	http	66.186.184.204	25.5 Mb

Scrutinizer - Top Interfaces v1.2512

Dev	Interface	Inbound	Outbound
N5	1 - to Skow-DHS-DOL S3/1 (Serial0/0)	17.201%	3.954%
S5	1004 - Alcatel 1/4 6.1.2.110.R03 (1/4)	0.051%	1.944%
S5	2 - Summit48si-Port 2	0.094%	1.020%
S5	1 - Summit48si-Port 1	1.020%	0.134%
S5	1001 - Alcatel 1/1 6.1.2.110.R03 (1/1)	1.015%	0.092%

Scrutinizer - Recent Alarms v1.2512

Alarm	Count	First	Last
Possible worm attack originating from 24.39.1.172 on name:downloads.somix.com address:24.39.1.172 Interface:(4) shows a VIOLATION of 71 RSTACK packets in a 5 minute period The limit is 40.	322	03/04/2008 10:14PM	03/06/2008 2:44PM
Possible worm attack originating from 66.186.184.195 on name:Solon-DOT address:66.186.191.226 Interface:Nu0(3) shows a VIOLATION of 122 RSTACK packets in a 5 minute period The limit is 40.	74	03/06/2008 6:24AM	03/06/2008 2:44PM

Scrutinizer - Google Map v1.2512

Map - Bercs Group v1.2512

104.42 ms

1.015%

4.34

2.76



## Scrutinizer NetFlow and sFlow Analysis

Scrutinizer is a NetFlow and sFlow analyzer that provides incredibly detailed network utilization information about the users and applications that are on the network. Using both Cisco's NetFlow Technology (an IOS software feature found in an ever increasing number of switches and routers) and industry standard sFlow, Scrutinizer is able to retrieve the traffic details you need and present them in a detailed graphical view.

## Distributed Analysis using existing routers

Learn all the above without deploying probes. Scrutinizer taps into functionality already possible with your existing equipment. Just enable NetFlow or sFlow on your existing routers and point the flow to the machine Scrutinizer is installed on. Then, from any web browser, gain tremendous insight into the traffic patterns on your network. Quickly gain details on *who*, *what*, *when* and *where*.

You may be surprised what you find.

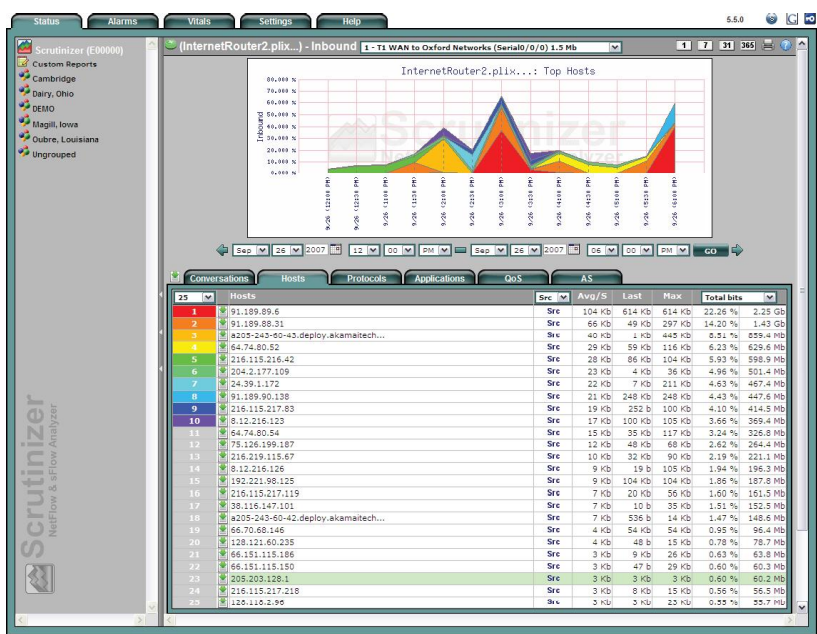


Figure 1: Top Hosts

## Learn from Scrutinizer

- What are the user traffic trends for certain applications?
- How much VoIP do you have on your network and who is involved with the most calls?
- What traffic could benefit from prioritization?
- What are the systems involved with a virus?
- Why are certain servers communicating using strange protocols?
- What applications are having the largest impact on the infrastructure?

## How it works

Most major switch and router vendors support technologies called NetFlow or sFlow. Vendors include: Cisco, Enterasys, Extreme, Foundry, Juniper, Riverstone, Packeteer and dozens of other vendors. Once Scrutinizer is installed on a computer, configure the switches to send the NetFlow or sFlow information to Scrutinizer. In just a few minutes, you will have traffic details from several geographically disparate locations on your network.

"We have been using another product, but I use Scrutinizer on a large network. It's an invaluable tool for determining the "who, what, and where" of network activity. Scrutinizer is a world-class product with an intuitive and easy-to-use interface. It's feature rich and a much lower cost than other NetFlow management products."  
- State of Maine

"I started using the freeware version of this new tool and I must say it's already been helpful. It takes the per packet info from the NetFlow streams you configure on your Cisco router and displays it in an easy to use web interface. I've known how much traffic I had on my interfaces, but didn't know what the content of the traffic was. I was able to identify the cause of a network link running slow because of one user transferring a huge file during the day over a slow link. Scrutinizer saved me a lot of time troubleshooting the old fashion way!"  
- Central Maine Power

We deliver the tools you need...

Plixer International, Inc. designs, develops and services NetFlow products and solutions for small and medium sized businesses. Our technical support and installation services ensure that every installation works with your existing software investments.

## Minimum Hardware Specifications

- Windows 2000/XP/2003
- 2 Gigs of RAM
- 15,000 RPM IDE or SATA Hard Disk
- 2 GHz+ processor
- Minimum 100 Megs of hard drive space for program files
- Minimum 300 Gigs of hard drive space for database files



### Scrutinizer helps remove the guess work

Scrutinizer will quickly become one of the first tools you reference when the boss asks, "Why is it so slow?" Scrutinizer's "Simple Flow Guide™" will lead you from a high level interface down to a specific router, interface, user, application. Incredibly FAST!

### Easy Reports

Built around a fundamentally simple design philosophy, Scrutinizer's learning curve couldn't be shorter. From specifying time frames with Drag & Drill™ or locating specific hosts with the Host Search, everything just makes sense.

### Custom Reporting

Custom Reports will allow the user to configure very detailed reports:

- IP Addresses, ranges and subnets
- Port numbers and ranges
- Defined Applications which include ranges of protocols
- Combine interfaces from multiple routers
- Specify bandwidth for the combined interfaces
- Scalable interface for hundreds of routers
- Security support for service providers wanting to give customers access to only specific data

### Service Levels

Scrutinizer allows you to verify application availability while simultaneously letting you review traffic levels. For example, you can see if several people were, in fact, getting their email.

### Conversation Reporting

Scrutinizer allows users to view conversation information being transferred between hosts. This is useful in determining not only what hosts are talking to each other the most, but what protocol is being used as well.

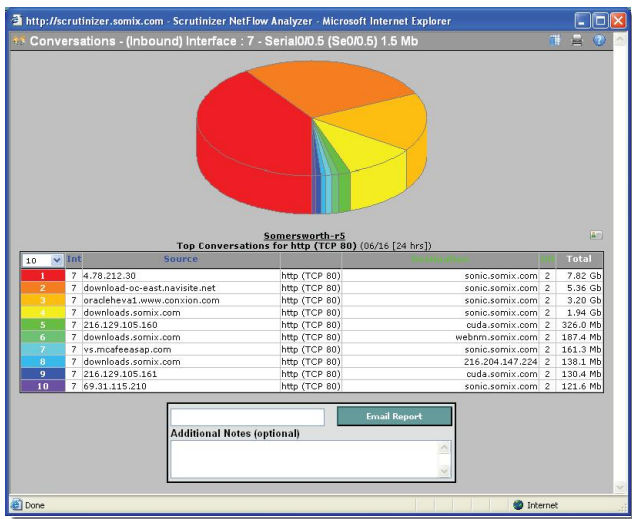
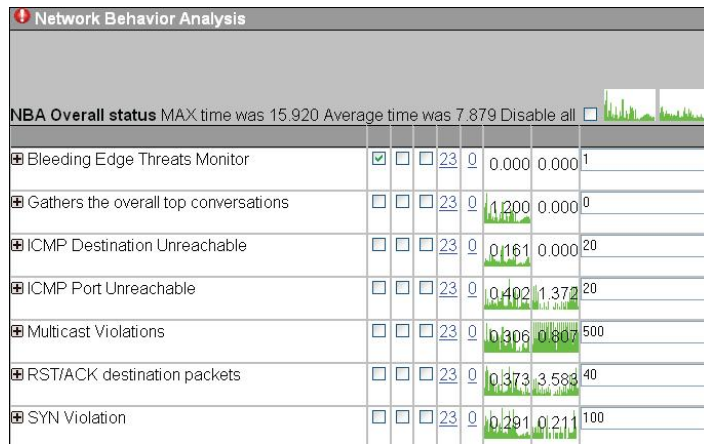


Figure 2: Conversation Reporting

If it is more top level conversation reporting that is needed, Scrutinizer provides any easily accessible interface that gives high level information on the top conversations getting saved.



Event	Enabled	Alert	Count	Max	Avg	Min
Bleeding Edge Threats Monitor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	23	0	0.000	0.000
Gathers the overall top conversations	<input type="checkbox"/>	<input type="checkbox"/>	23	0	1,200	0.000
ICMP Destination Unreachable	<input type="checkbox"/>	<input type="checkbox"/>	23	0	0,161	0.000
ICMP Port Unreachable	<input type="checkbox"/>	<input type="checkbox"/>	23	0	0,402	1,372
Multicast Violations	<input type="checkbox"/>	<input type="checkbox"/>	23	0	0,306	0,807
RST/ACK destination packets	<input type="checkbox"/>	<input type="checkbox"/>	23	0	0,373	3,583
SYN Violation	<input type="checkbox"/>	<input type="checkbox"/>	23	0	0,291	0,211

### Network Behavioral Analysis

Scrutinizer uses behavior algorithms to automatically alert you when trouble is recognized to be outside of normal traffic patterns. It detects:

- Zero -day worms, SYN Floods and DoS attacks
- Policy violations and internal misuse
- Poorly configured and unauthorized devices
- Unauthorized application deployments

### Real-Time Data

Scrutinizer is the world's first real-time web-powered NetFlow and sFlow tool. Its architecture scans thousands of conversations per minute and extends information in an easily comprehensible format.

The following NetFlow information is captured in real-time:

- Top Applications and Hosts
- Top Applications per Host
- Top Hosts per Application
- Top Conversations
- Top QoS and Autonomous Systems

Scrutinizer can also show a real-time SNMP trend of each interface's utilization. Watch traffic flowing through a link as it is happening.

### Historical Trending

The Scrutinizer "Intelligent Interval Retrieval Architecture™" saves detailed data for unlimited years in many formats, which gives you the data to look back and see trouble spots.

### Application Grouping

Sometimes applications can use a number of different protocols. Scrutinizer allows users to specify ranges of protocols and group them as a single type of application.

### VoIP Analysis

Voice over IP (VoIP) Analysis is assisted by Scrutinizer by verifying:

- How much voice traffic is historically on the connection
- What devices are involved with the most VoIP traffic

**Visualize Global Networks with Google Maps**  
Scrutinizer offers advanced integration with the Google Maps API, which allows users to plot routers, switches and device groups on an imbedded Google map. This helps make high level network navigation a snap and provides a window into your Scrutinizer details.

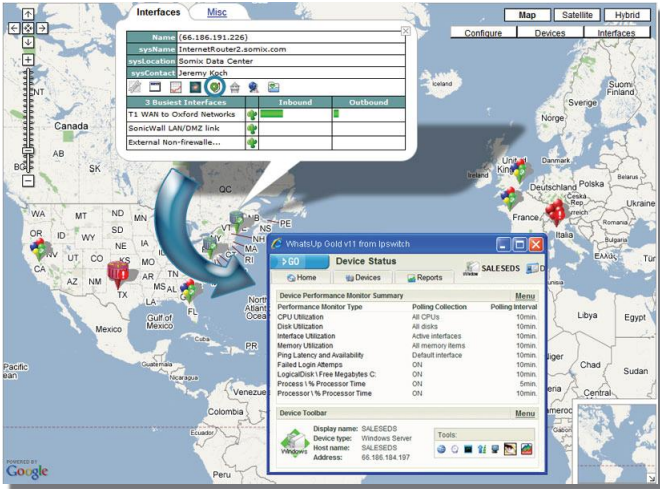


Figure 3: Google Maps

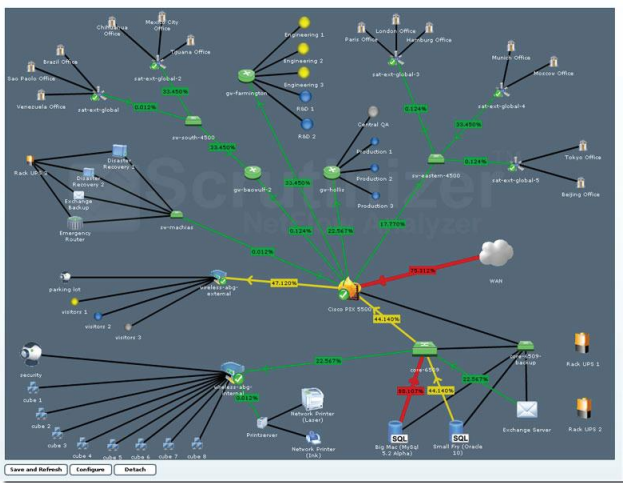
Zoom in on your country, state, city or street and see what devices are down. Looking for more details? Click on a device and see a snapshot of the three busiest interfaces on that router or even jump over to a custom link or third party application (e.g. Solarwinds Orion, WhatsUp Professional, SNMPc, etc.) for that host address. Click on a device group to dive into a customized network map you create.

**What You See is What You Get**

**Interactive Network Maps**

Maps come to life in Scrutinizer where links change color and thickness based on utilization, and clicking on links brings up the top talkers and conversations within the last minute!

Figure 4: Network Mapping



These completely customizable maps are managed entirely through a web browser.

With Scrutinizer's new Network Mapping utility:

- Maps are 100% configurable via a web browser
- Drag icons in the web interface and save settings if permissions allow
- Create links to other favorite 3rd party applications
- Click on flow devices and bring up the top interfaces on that device
- Create high level maps with links to other maps that indicate status
- Integrates with Google mapping architecture
- Put a single device in multiple maps (i.e. groups)
- Status of icons based on whether NetFlow is being received
- Syslogs sent if interfaces go down or if utilization hits a threshold
- Links change color and thickness based on utilization and the arrow represents the direction

If it is more top level conversation reporting that is needed, Scrutinizer provides any easily accessible interface that gives high level information on the top conversations getting saved.

**Device Grouping**

Categorize devices and routers into logical groups that can be placed on your Google maps or explored via the Scrutinizer tree menu. Click on the device group icons to zoom into an interactive Scrutinizer network map.

Device groups can contain any kind of network device, as well as links to other device groups and third party applications.

**User Management**

Manage accounts by assigning access to custom reports, device groups, network maps and Google maps to individual users. Administrative privileges and user access is not the same thing. That's why Scrutinizer allows admins to determine who can view what information, as well as who can make configuration changes.

Service providers can limit their customers to only seeing maps and device groups that are appropriate for them.

**QoS (ToS and DiffServ) Support**

Verify that the traffic on the network is prioritized with the correct tags. Scrutinizer can identify miss tagged applications requesting priority throughput and even display the hosts involved.

**The Best Value in NetFlow**

Regardless of your reason for choosing Scrutinizer, you'll easily recognize the value it brings to your network equipment and your team.

Scrutinizer supplies the information necessary for administrators to troubleshoot most network congestion problems and keep the network links running at peak performance.