Release Notes

Scrutinizer

SonicWALL Scrutinizer 9.0.1 Release Notes

Contents

System Requirements

Scrutinizer 9.0.1 is supported on systems with the following:

Minimum System Requirements (for trial installations)

- 4GB RAM
- 50 GB IDE or SATA Hard Disk
- Dual Core 2GHz+ Processor
- Windows Vista / 2008 / 7 Operating System

Recommended System Requirements (for production environments)

- 8GB RAM
- 1+ TB 15k SCSI in a RAID 0 or 10 configuration Hard Disk
- Quad Core 2GHz+ Processor
- Windows 2008 Server

Enhancements in SonicWALL Scrutinizer 9.0.1

Scrutinizer version 9.0.1 introduces the following new enhancements:

- Denika Threshold Policy
- NBAR Application Latency Reports
- Open Source Method Back Up
- Custom Template ID Added in the Available Reports List
- Chinese Localization
- Business Hours Reports
- Device IP Callouts
- Command Line Reset

Key Features in SonicWALL Scrutinizer 9.0

The following enhancements are new in the SonicWALL Scrutinizer 9.0 release:

- **Enhanced Notifications and Facilitation of Automatic Remediation:** In version 8.6 and earlier versions, Scrutinizer only sent syslogs. Version 9 adds the ability to send notifications and escalate issues. If the first person notified doesn't clear the alarm within a given time period, a second person, third person, and so on can be notified via email, pager, and other options listed below.

  Notifications can be sent when alarms are triggered based upon specific SonicWALL firewall security related events.

  New notification options include:

  1. Email notifications about network activity can be sent to administrators using mobile and other devices.
  2. SNMP Traps can be triggered allowing for greater integration with existing notification options.
  3. Syslog Messages allow for greater remediation when integrated with third party SIEM products such as ArcSight.
  4. Script execution allows for automatic remediation eliminating the need for manual intervention.

  Scrutinizer now facilitates automatic remediation based on specific events: Previous versions of Scrutinizer, as do most other third party flow analytic applications, only provide messages to the user when alarms are triggered. By adding SNMP Traps & Script Execution, Scrutinizer now has the potential to remediate events.

  For example, SonicWALL IPS sees an attack occurring on the LAN, an alarm in Scrutinizer is triggered which in turn sends an SNMP Trap to the Cisco switch to shut down the interfaced being used in the attack.

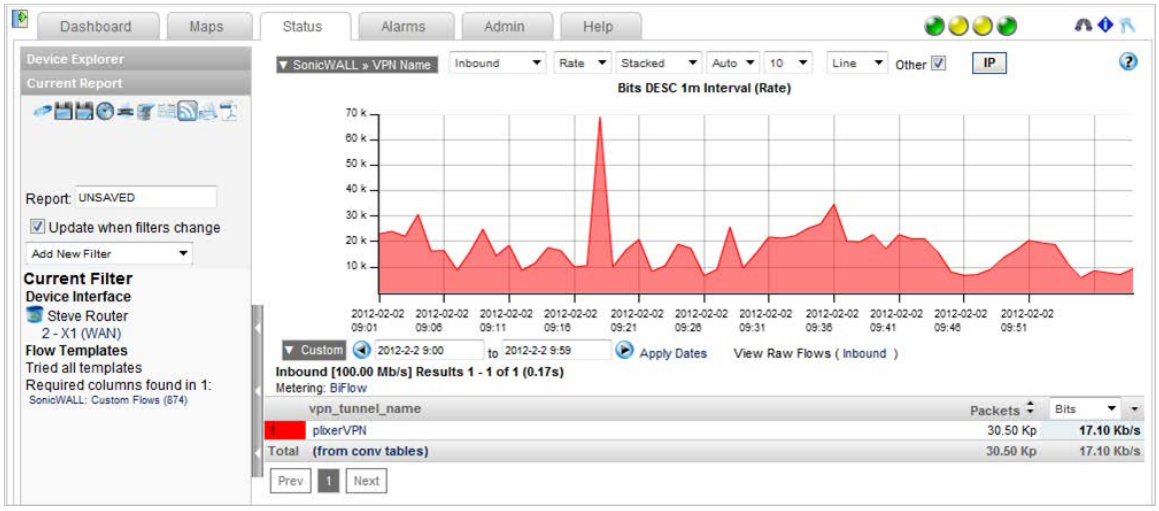
- **Advanced SonicWALL VPN Reporting** with granular drilldown capabilities including:

  Reports are available for both site-to-site VPN connections and remote user IPSec VPN connections, i.e. Global VPN Client connections

  User Details include user name, authentication method, and domain for detailed reporting on specific users.

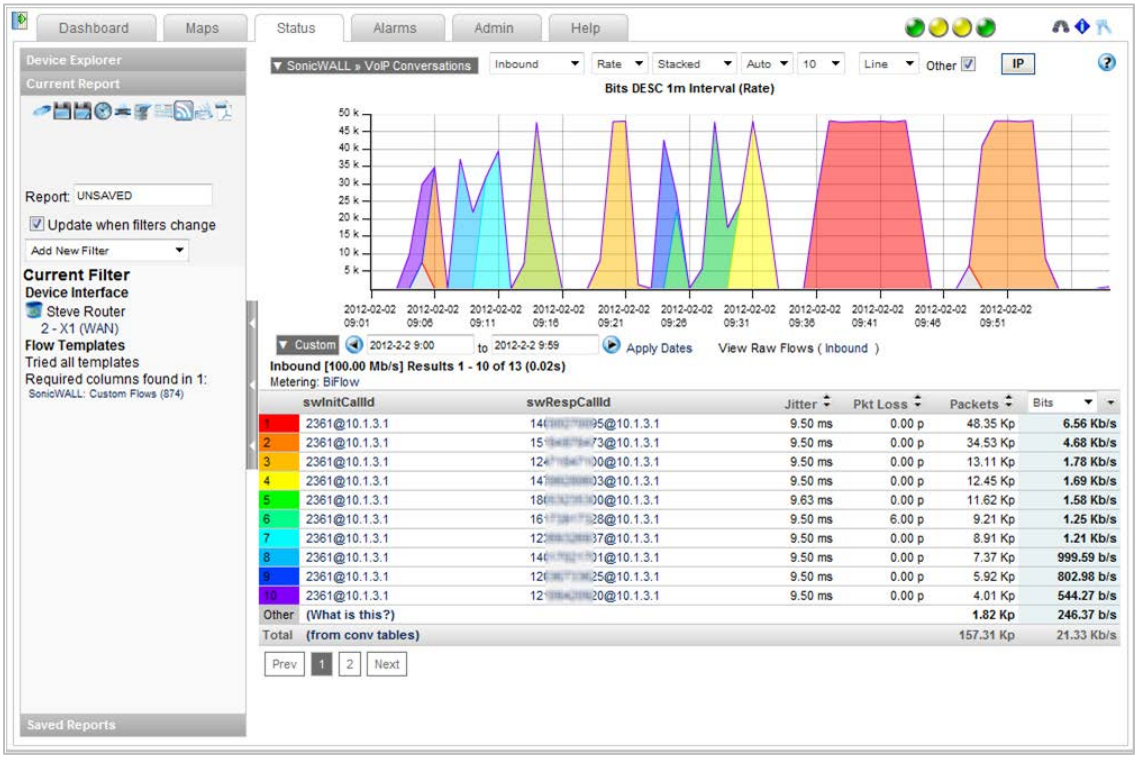
  Reporting data can be cross referenced with the friendly VPN name, the remote system's IP address and the local system's IP address.

New SonicWALL Scrutinizer VPN Report Type



- **Enhanced SonicWALL VoIP Reporting** including:
  - SonicWALL VoIP conversations reports have been optimized.
  - SonicWALL VoIP call filtering now allows for partial text matching.

Enhanced SonicWALL VoIP Conversation Report



SonicWALL VoIP Call Filter Now Supports Partial Text Matches

- **Enhanced Cisco Reporting** in support of recently introduced Cisco technologies:

  Smart Logging and Telemetry (SLT) is a single mechanism of logging and telemetry of traffic that is associated to a specific event on a switch (for example, an event triggered by an ACL-permitted or ACL-denied packet). SLT is a threat detection technology and is intended to be used as follows. An admin will configure one or more Access Control Lists (ACL) on the switch. If an end system violates an ACL, some of the packets will be captured and sent off in a NetFlow datagram with the name of the ACL that was violated. Scrutinizer version 9 can collect and report on these NetFlow messages.

  Cisco TrustSec (CTS) is an umbrella term for security improvements to Cisco network devices based on the capability to strongly identify users, hosts and network devices within a network. Each CTS Group is a secure network establishing a domain of trusted network devices. Every device in the Security Group Access (SGA) domain is authenticated by its peer device. Communication on the links between devices in the SGA domain is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. NetFlow reporting allows administrators to monitor the traffic from, and between, the different CTS groups.

  Performance Routing (PfR) complements traditional routing technologies by using the intelligence of a Cisco IOS infrastructure to improve application performance and availability. PfR enhances routing in order to select the best path based on user defined policy. The PfR policy can minimize cost efficiently by distributing traffic load and/or selecting the optimum performing path for applications. PfR NetFlow reports provide details on active and passive traffic. Active traffic is where the router makes routines connections and exports the performance results, e.g. out of policy, in NetFlow. Passive traffic can also be monitored and measured for performance and metrics are exported in NetFlow.

  MediaNet Performance Monitoring reports on top interfaces with the most jitter/latency.

  All these features require the Cisco Advanced Reporting Module.

New Host Destination Report

- **Advanced Citrix Reporting** with granular drill down capabilities including:
  - o URLs providing reporting insight into web servers and databases being accessed
  - o Applications providing reporting insight into applications being accelerated via NetScaler
  - o Latency providing reporting insight into the health and delay as seen by NetScaler

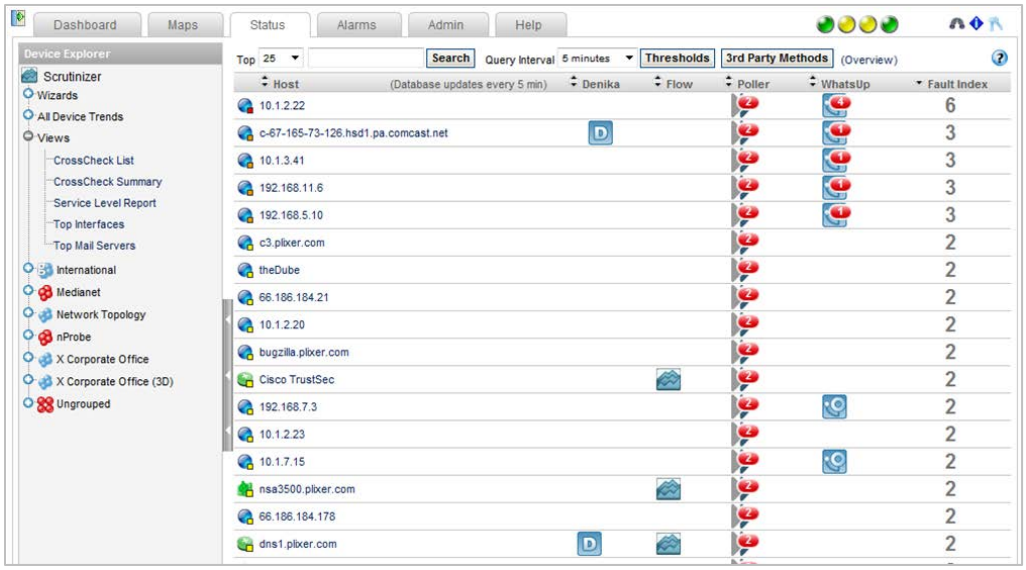
  Note: Citrix NetScaler makes applications and cloud-based services run five times better by offloading application and database servers, accelerating application and service performance, and integrating security.

  All these features require the new Citrix Advanced Reporting Module.

- **Device Overview Dashboards** provide details on the host status and outstanding alarms
  - o Gadgets can be imported including the real-time view of application usage screen in SonicOS
  - o Service Level Report list availability and latency trends on all devices polled

- **Scrutinizer Cross Check** provides integration with third party monitoring and flow analytic tools such as WhatsUp Gold, Orion, SNMPc, Uptime Devices and Nimsoft. This new module's capabilities include:
  - o Cross Check creates central inventory of all network devices managed by other analytic tools displaying several attributes including device name, IP address, and status.
  - o Flowalyzer Poller continually assesses the status of devices identified by Cross Check and provides updates to Scrutinizer via IPFIX messages.
  - o Cross Check references the status of devices as known by Scrutinizer with other third party management products to monitor if flow data is arriving properly and whether devices are being polled correctly
  - o Fault index measurements indicate device status across numerous management systems using configurable severity levels. Syslog notifications can be sent out if predefined threshold levels are met.
  - o Clickable inventory allows users with direct links to integrated third party applications providing easy access to devices that are managed via these other applications.
  - o Inventory groupings can be created allowing for easy monitoring of network segments regardless of whether the appliances are managed by Scrutinizer or a third party application.
  - o Cross Check was created directly in response to large MSP and enterprise customer demands for third party integration.

  All these features require the Cross Check Module.



- **Improved SonicWALL report searching capabilities**--It is now possible to search on portions of a URL rather than the exact URL

Scrutinizer Product Overview

SonicWALL Scrutinizer is a network traffic monitoring, analysis and reporting tool. Scrutinizer is a mature and feature rich flow analytic platform.

Scrutinizer is used to monitor the overall health of the network, troubleshoot irregular network traffic patterns and optimize network performance. The Scrutinizer application is run on a Windows server and accessible through a web-based Graphical User Interface (GUI). IT administrators use SonicWALL Scrutinizer to collect, monitor, and analyze data on user and application usage across the network. Scrutinizer provides administrators with great insight into *how* the network is being used through the use of highly customized granular reporting. Administrators can be alerted based upon a set threshold or on a pre-determined schedule.

Scrutinizer supports a wide variety of flow protocols allowing compatibility with virtually every collector available in the market today. In addition to SonicWALL's pioneering IPFIX implementation in SonicOS 5.8+, Scrutinizer also supports Cisco's Flexible NetFlow. Customers utilizing Scrutinizer receive even greater value for their investment as the software can be utilized to monitor an ever increasing number of switches and routers, due to support for numerous additional industry standards such as NetFlow v5, NetFlow v9, sFlow and J-Flow. Additional supported hardware vendors include Enterasys, Foundry, Juniper, Riverbed, VMware, Citrix, ADTRAN, Nortel and many others.

Supporting a broad range of network devices, flow protocols, and application types, Scrutinizer is flexible enough to be utilized on virtually any network. Administrators are able to leverage reports to reach a level of visibility previously not possible. The network mapping feature allows administrators visibility into almost every link on the network greatly enhancing troubleshooting efforts. Scrutinizer's powerful analytics engine provides users with in-depth traffic analysis which was previously only available through packet-based instrumentation. Advanced analysis algorithms and premier industry usage of IPFIX and NBAR based technologies are at the core of Scrutinizer's impressive set of application level reporting and alerting capabilities.

Scrutinizer is a free tool for download by any IT professional. Three of the main limitations of the free product are that it:

- only stores a maximum of 24 hours of data
- does not include most SonicWALL specific reports
- can only support up to five devices

For the first 30 days after installation, the free Scrutinizer product includes the Flow Analytics Module. To make use of the features available in the Flow Analytics Module beyond the first 30 days, you have to purchase and activate a Flow Analytics Module license.

There are five optional add-on modules for Scrutinizer which are sold separately: the Flow Analytics Module, the Service Provider Module, the Cisco Advanced Reporting Module, the Citrix Advanced Reporting Module, and the Cross Check Module.

Scrutinizer Base Product

The base Scrutinizer product includes many great features such as:

Administration

- Customizable Dashboards
- Group Based User Permissions
- Unique Dashboards per login

With Scrutinizer's suite of built-in administrative tools, customizing specific user logins and dashboards is a breeze. Administrators can create specific permissions based upon a particular user identity or create group based user permissions for entire departments. The Dashboard can be customized on a per-user basis to provide the information that is most relevant to each user upfront.

Alerting

- Support for on-demand email reporting
- Ability to batch schedule and email reports to administrators

Scrutinizer was built with ease of use in mind. With Scrutinizer's alerting features administrators have 'set it and forget it' flexibility when it comes to reporting. Reports can be run based upon a specific schedule or triggered when event thresholds are exceeded. Once configured, reports can be automatically batched and emailed to administrator in several formats.

Flexible Reporting

- In the Free version, data can be archived for up to 24 hours. Data can be saved longer if a commercial version is purchased.
- Extensive Flexible NetFlow template support
- Granularly defined reports down to the second which can include / exclude data filters
- Create and save templates to easily reuse for future reporting
- Create application group reports based upon specific ports or subnets
- Display data by number of bits, bytes, packets or as a percentage of total traffic
- Per interface, host, protocol, application, or conversation reporting
- Trend data in, out, or bi-directionally

Granular, flexible reporting is the heart of the Scrutinizer product. Administrators have endless possibilities for generating reports based upon general or very specific criteria. Want to know which users are consuming the most bandwidth? Would you like that done per bit, byte or packet? What about which protocols are being most heavily utilized on a particular subnet?

Security

- Easily configure DNS caching time limits
- See all traffic 'Host to Host' or 'Subnet to Subnet'
- Easily filter and display traffic based upon TCP flags
- Track flow sequence numbers to trend traffic patterns
- Quickly identify MITM servers on the network (DNS, DHCP, SMB, etc)

With all of these great features it's no wonder Scrutinizer is invaluable when it comes to security. Administrators can toggle between various reports to easily identify traffic flowing from host to host or subnet to subnet. Tracking flow sequence numbers and trending traffic patterns has never been easier. Further, Scrutinizer can quickly identify rogue servers placed on the network attempting a Man-in-the-Middle attack against such services as DNS, DHCP, SMB, and more.

Supported Protocols & Other Technical Specifications

- Granularly define reports down to specific interfaces across multiple routers, switches, or firewalls
- Easily integrate 3rd party application and URLs into dashboards
- Integrates with LDAP servers
- Support for SNMPv1, SNMPv2c, and SNMPv3
- Support for all industry standard flow analytics (IPFIX, NetFlow v5, NetFlow v9, FnF, sFlow, J-Flow)
- Configurable to over 1000 interfaces and several hundred exporters
- Create filters based upon next routing hop
- Filter on any exported field such as VLAN id, L2 Address, L3 Address, and latency
- Immediate cost savings by not requiring the purchase of an expensive Microsoft Database server
- Capable of handling up to 20,000 flows per second on an unlimited number of UDP ports

From a technological stand-point Scrutinizer leaves similar priced flow analyzer products in the dust. Scrutinizer's robust and superior features such as LDAP integration and support for every industry standard flow protocol in the market today provide enormous value. When configured appropriately the Scrutinizer engine can receive up to 20,000 flows per second on over 1,000 different interfaces. Customizable dashboard 'mashups' allow for 3rd party applications and URLs to be imported directly into Scrutinizer making it the only application needed to know exactly what's on the network.

Troubleshooting

- Easily identify link failures
- Easily identify specific link traffic statistics
- Easily identify QoS across the network by analyzing jitter & latency
- Easily find out where the 'slowness' on the network is occurring
- Plan for network growth

Administrators can use Scrutinizer to monitor the volume of traffic on their network and analyze how it is fluctuates over time. In fact, Scrutinizer's 'network volume gadget' feature can be utilized to see the number of unique hosts and well known applications being accessed. This report shows trending information on the number of hosts accessing the network providing the IT administrator with insight into increases over time. Additionally, reports can be limited by time range (such as 9am to 5pm) to monitor network traffic volume during peak business hours.

Scrutinizer can also be used to identify bottlenecks on the network. For example, when streaming video or VoIP is deployed on the network, automatic alerts could be configured in Scrutinizer to email the IT administrator notifying him of packet-loss, delays in packets arrival, or packets arriving out of order. This provides an IT admin the ability to proactively know of call quality degradation even before users complain of an issue.

Visibility

- Trend analysis reports on archived data
- Easily see the top 5 interface across all routers, switches & firewalls
- Integrated Google Maps viewing allows for visual representations of distributed network
- Flexible viewing options allow data to be seen from different angles (pie, bar, matrix, line)

Various viewing options within Scrutinizer, such as the matrix view provide an innovative tool for better visualization of traffic flows. Based on criteria established when the report is generated, administrators can toggle to different views to see a graphical map of where traffic is flowing. The 'Matrix' enables administrators to easily visualize which systems a particular host has been accessing.

Flow Analytics Module

The Flow Analytics Module brings traffic flow diagnostics to the next level by adding historical reporting for an unrestricted period of time, advanced alarming with the ability to set thresholds, role-based administration, and in-depth traffic analysis algorithms to the Scrutinizer software. It can easily identify top applications, conversations, flows, protocols, domains, countries, and subnets on the network, as well as watch for and alert on suspicious or potentially hazardous network behavior patterns thereby providing administrators with greater network security awareness.

In addition to the base-level features Scrutinizer with the add-on Flow Analytics module provides several additional advanced features, such as:

- Flexible Reporting
  - SonicWALL specific templates for reporting
  - Special traffic analysis reports such as Flow Volume & NBAR Support
  - MPLS reporting by subnet
  - Microsoft Exchange log trend analysis
  - Puts information at administrators fingertips
    - Easily identify the top applications being utilized on the network
    - Easily identify the top country of origin for traffic flowing across the network
    - Easily identify the top domains being accessed
    - Easily identify the top subnets being utilized on the network

With the addition of the Flow Analytics module Scrutinizer becomes an even more powerful reporting engine offering even greater flexibility and granularity. In addition to all the reporting functions provided in the base edition, Scrutinizer with Flow Analytics adds advanced reporting options such as flow volume, MPLS by subnet, Microsoft Exchange log trending and NBAR support. Administrators have with a wealth of information right at their fingertips. IT administrators can create custom reports by applying filters to granularly define the specific information desired. Once created, custom reports can be saved for later use. Custom Reports allow the user to configure detailed reports by filtering on fields such as: IP Addresses, ranges and subnets; Port numbers and ranges; Defined applications including ranges of protocols and groups of protocols; Multiple interfaces from different routers and switches; Any exported field available via NetFlow or IPFIX; Dynamic QoS monitoring; Detailed security / forensic information

The Flow Analytics Module adds several additional flow based traffic analysis report types. Examples include but are not limited to: Granular IPFIX based application visualization reports for SonicWALL products; Flexible NetFlow NBAR based application reports (requires IOS v15 on Cisco routers); Conversations to/from host pairs and applications used; Flow reports with ToS field; Host flow reports to show hosts sending or receiving the most flows; Host volume reports to show the volume of unique hosts per second; Pair volume reports to show the volume of unique to/from address pairs per second

- 'Set It & Forget It' Alerting
  - Easily create alerts to notify administrators of unfinished flows or nefarious activities
  - Alerts can trigger email notifications, SNMP traps, syslog messages, and script execution (facilitating event remediation)
  - Alarms can be configured to alert administrators based upon specific interface utilization
  - Administrators can be alerted based on any pre-defined report
  - Reports can be scheduled, then emailed to administrators
  - Administrators can proactively monitor QoS of RTSP traffic

The Flow Analytics add-on to Scrutinizer provides administrators with greater automation control making routine advanced reporting a snap. Alerts can be configured based upon everything from unfinished flows to specific interface utilization. Further, administrators can configure QoS thresholds to proactively be alerted of RTSP latency and jitter before end users even reports a problem.

Using saved Scrutinizer reports, the Flow Analytics Module can monitor and send out syslogs when traffic patterns violate specified thresholds. For example, the Flow Analytics Module can be used to monitor an application for a certain ToS within a class A subnet.

- Enhanced Security Awareness
  - Administrators can create a list of banned applications to be alerted upon traffic identification
  - Detect malicious traffic such as DDoS attacks, worm traffic and more
  - Detect numerous types of network scans such as SYN, XMAS & FIN
  - Detect rouge IP addresses that lie outside of predefined subnets

The enhanced security functionality alone makes Scrutinizer with Flow Analytics an invaluable tool in an administrator's arsenal. Know exactly what is happening on the network- where traffic originated, where it is going and what type of traffic it is. Is someone planning an attack by scanning the corporate network? Did one of the servers get infected with malware and launch a DDoS attack? Scrutinizer can automatically detect these activities and alert administrators immediately upon detection.

At the heart of Scrutinizer's attack detection capabilities are a behavioral analysis engine and a periodically updated known threats database. IT administrators can use Scrutinizer to identify and alert on threats such as DDoS attacks, port scanning, attacks from infected hosts behind the firewall. In turn this allows the administrator to remediate threats by making configuration changes, such by disabling ports, and modifying ACLs, on routers, switches and firewalls. Scrutinizer uses configurable algorithms to analyze flow data from the entire network infrastructure, or from a pre-configured sub selection of devices and exporter tables to automatically send syslog messages when trouble arises. Using Scrutinizer IT staff can identify: RST/ACK worms, zero-day worms, SYN Floods, DoS, DDoS attacks, NULL, FIN, XMAS scans, port scanning, P2P file sharing, Excessive ICMP unreachable, Excessive Multicast traffic, Prohibited traffic being tunneled through allowed protocols (DPI on TCP port 80), Known compromised internet hosts, illegal IP addresses, Policy violations and internal misuse, Poorly configured or rouge devices, Unauthorized application deployments

The Flow Analytics Module can utilize the local DNS to resolve IP addresses in real-time. This allows Scrutinizer to group traffic into domains without having to define ranges of IP addresses which could otherwise quickly become a nightmare to manage. With this feature, Scrutinizer can be configured to monitor traffic to or from specific domains and alert an administrator when preconfigured thresholds are met or exceeded.
The history of repeat offenders can be easily identified through the use of a Unique Index (UI) to manage traffic counts. In addition, the Flow Analytics Module helps locate machines involved with DDoS attacks or infected with viruses/worms.

The Flow Expert Window provides insight to immediate network problems as they occur to identify and resolve DoS attacks, bottlenecks, network scans, improperly terminated connections and more. Traditionally, the functionality provided by this "Expert Window" feature has only found in packet analyzers.

- Supported protocols & other technical specifications
  - Support for L7 application awareness by using NBAR or IPFIX
  - Automatic DNS resolution

Tired of looking at a list of meaningless IP addresses? Wouldn't it be great if the flow-analyzer could perform reverse DNS lookups on those addresses in real time? Want to know what specific Web 2.0 applications are being accessed on the network? Scrutinizer with the Flow Analytics module can do all that. Administrators running Flexible NetFlow with NBAR or IPFIX with extensions can easily identify applications such as YouTube, Facebook, eBay and more instead of just seeing 'TCP port 80' on the report.

Advanced Troubleshooting

- Begin capacity planning for growing networks
- Easily identify the volume of flows per host
- Easily identify the volume of traffic flowing between a pair of hosts
- Easily identify the volume of unique hosts per second traversing the network
- Peer into VoIP traffic when using IPFIX to see granular metrics such as codec & caller ID

  IT administrators can use Scrutinizer to analyze Voice over IP (VoIP) traffic and determine: the amount of voice traffic into and out of the network over time; what users are involved with the most VoIP traffic; the caller ID of destination and source; QoS statistics such as Latency/Jitter and packet loss of each call; what audio codec is being utilized; and whether the router is modifying DSCP values.

By using multiple servers to act as distributed flow data collectors, Scrutinizer can be deployed as a distributed solution accessible through a single central web based interface allowing for easy scalability to support enterprise level networks.

Dozens of distributed collectors can be deployed and, depending on the volume of flow data being received by each collector, a single deployment of Scrutinizer can potentially support hundreds of firewalls, routers and switches.

Network topology maps come to life in Scrutinizer as links change in color and thickness with variations in network utilization. Clicking on a link in a network topology map brings up useful traffic statistics such as top talkers and top conversations within the last minute.

IT administrators can use Scrutinizer to plot network appliances such as firewalls, routers, and switches on a Google map embedded in the Scrutinizer application. Using this geographic map as a starting point into all network analysis provides traffic details collected and organized for easy visualization in Scrutinizer

Service Provider Module

The Scrutinizer Service Provider Module adds several additional features which are especially useful for Managed Service Providers (MSPs) and Internet Service Providers (ISPs). The following are some important features included in the Service Provider Module:

- Ability to easily modify style sheets, i.e. to change the logos, colors and fonts, to match the Service Providers marketing and branding efforts. To further facilitate this, several default style sheets have been included with the product.
- Ability to configure permissions per router, switch, or interface for each Scrutinizer login account.
- Ability to customize a default landing page for end customers that require access to Scrutinizer.
- Ability to integrate with third party applications, URLs, and mashups.
- Customizable billing solutions based on actual network usage for invoicing purposes. Ability to export reports to .CSV format for easy importing to a database or MS Excel.

Third Party Product Integration

The Scrutinizer dashboard function includes a URL mashup feature to provide third party application vendors and professional services organizations a comprehensive yet easy method to access information within the Scrutinizer database.

Mashups, representing a combination of information from several different applications into a single easily accessible dashboard, is a new class of short-term or disposable applications which can be created quickly and easily. Utilizing simple web technology, Scrutinizer allows anyone to easily assemble a URL into such a mashup or third party application to directly import and display important information regarding the activity of a specific host or application on your network.

Scrutinizer integrates with several third party and open source applications.

Enablement of Traffic and Usage Based Billing

Some customers request to be billed for their Internet connection not based on a theoretical maximum throughput of their connection but rather on actual usage. To accommodate this customer demand, service providers have to be able to determine actual bandwidth usage in order to bill each customer accurately and fairly.

The Scrutinizer Service Provider Module allows service providers to export flow data based on any flow (NetFlow, IPFIX, sFlow, etcetera) field or combination of flow fields including rate per second, packets, total bits, IP addresses, ToS (DSCP), or BGP autonomous system number. This data can then be used to invoice end customers based on actual network usage rather than simply WAN connection speed.

The Service Provider Module routinely exports a custom CSV file with all the required details. For example, it allows billing based on a flat rate versus a burst rate as well as total amount transferred per month. With the data export, invoicing possibilities are myriad. Invoices can include, but are not limited to:

- A fixed amount for any usage within the base rate (X MB)
- A higher charge for usage between the base rate and “burst” max (X + Y MB)

More traditional billing is also possible, for example, where the end customer pays based on the 95% percentile technique.

Using the intuitive configuration interface, any saved report in Scrutinizer can become the basis for an export. To ensure the highest accuracy, data is gathered from the raw flow data tables. The Service Provider Module also includes the following capabilities:

- Any NetFlow field or range within a field is saved as part of the filter within a report.
- Both inbound and outbound flow analytics are available.
- The entire contents of any report type can be emailed or exported in CSV format.
- Archives of all exports can be saved for future reference.
- Exports occur on a periodic basis.
- Rolling the data into larger intervals is possible.
- Exports are emailed or saved in a directory with a custom name, which includes a time stamp.
- Scheduled routines:
  - Prepare the data for further processing
  - Can write the data to another server

Customer Portal

IT administrators can choose to provide end users are with secure login access to the flow data generated by their network devices. End users can also use the customer portal to troubleshoot bandwidth usage and identify / analyze odd traffic patterns. Additionally, automatic HTML reports can be scheduled for each end customer.

Furthermore, service providers can use the portal as a message board to communicate with their customers as well as integrate other applications into the MyView interface.

Cisco Advanced Reporting Module

The Scrutinizer Cisco Advanced Reporting Module is a value added performance monitoring and reporting solution for Cisco Smart Logging and Telemetry, Cisco TrustSec (CTS), Cisco Performance Routing (PfR), and Cisco Medianet. Scrutinizer delivers detailed reports on all traffic related to voice and video. IT staff can troubleshoot QoS issues related to choppy video or delayed voice streams by using Scrutinizer to analyze the appropriate flow.

Scrutinizer can be configured to analyze and alert on excessive amounts of one or a combination of the following parameters:

- Round Trip Time (Latency)
- Jitter
- Packet Loss
- Bits, Bytes and Packets
- MAC Addresses, IP Addresses
- VLANs
- Domains
- Applications
- Interface

Citrix Advanced Reporting Module

The SonicWALL Scrutinizer Citrix Advanced Reporting Module adds the granular drill-down capabilities for:

- URLs providing reporting insight into web servers and databases being accessed
- Applications providing reporting insight into applications being accelerated via NetScaler
- Latency providing reporting insight into the health and delay as seen by NetScaler

Note: Citrix NetScaler makes applications and cloud-based services run five times better by offloading application and database servers, accelerating application and service performance, and integrating security.

Cross Check Module

The SonicWALL Scrutinizer Cross Check Module provides integration with third party monitoring and flow analytic tools such as WhatsUp Gold, Orion, SNMPc, Uptime Devices and Nimsoft. This module's capabilities include:

- Cross Check creates central inventory of all network devices managed by other analytic tools displaying several attributes including device name, IP address, and status.
- Flowalyzer Poller continually assesses the status of devices identified by Cross Check and provides updates to Scrutinizer via IPFIX messages.
- Cross Check references the status of devices as known by Scrutinizer with other third party management products to monitor if flow data is arriving properly and whether devices are being polled correctly
- Fault index measurements indicate device status across numerous management systems using configurable severity levels. Syslog notifications can be sent out if predefined threshold levels are met.
- Clickable inventory allows users with direct links to integrated third party applications providing easy access to devices that are managed via these other applications.
- Inventory groupings can be created allowing for easy monitoring of network segments regardless of whether the appliances are managed by Scrutinizer or a third party application.
- Cross Check was created directly in response to large MSP and enterprise customer demands for third party integration.

All these features require the Cross Check Module.

Flowalyzer NetFlow & sFlow Tester

Separate from Scrutinizer and its add-on modules, SonicWALL also offers a free tool called Flowalyzer NetFlow & sFlow Tester.

Flowalyzer is a free NetFlow and sFlow Tool Kit for testing and configuring hardware or software to send and receive NetFlow / sFlow data.

Flowalyzer can help IT professionals troubleshoot hardware from vendors like Cisco and Enterasys, as well as NetFlow collector software, ensuring that whichever flow technology they use is configured properly on both ends.

Flowalyzer NetFlow & sFlow Listener

- Determine which flow sending devices are sending the highest volume.
- Listen for NetFlow on multiple ports.
- Display packet count, version of NetFlow and UDP port flows are coming in on.
- Display the IP address and DNS name.

Flowalyzer NetFlow Generator

- Generate NetFlow data to determine if the destination collector is accepting flows.
- Send NetFlow v5, NetFlow v9, and IPFIX.
- Determine if the destination collector is dropping NetFlow data by comparing the flows sent to what is received on the other end.

Flowalyzer NetFlow & sFlow Configurator

- Configure Cisco Routers or Enterasys switches for exporting NetFlow data
- Uses SNMP to make OID sets
- Supports SNMP v1, v2c, and v3

Flowalyzer NetFlow & sFlow Communicator

- Run a ping or traceroute to any host.
- Ping via ICMP, UDP or TCP protocols.
- Communication responses are readable in a clear response display.

Flowalyzer SNMP Trender

- Generate trend graphs for any SNMP-enabled device.
- Custom OID support allows any SNMP variable to be trended in real-time.
- Custom update period allows graphs to update as often as every second.
- Supports SNMP v1, v2c and v3.
- Save multiple sets of Read/Write SNMP credentials.
- No limit to the number of simultaneous graphs.

Known Issues

This section contains a list of known issues in the Scrutinizer 9.0.1 release.

Symptom	Condition / Workaround
MFSN report for some sFlow devices will occur even though no flows are being lost. This can happen if multiple subagents exist on a single sFlow exporter	Fix coming in a future release.
Flow Analytics can cause the server to page memory to disk and slow down the user interface. Generally, occurs on underpowered machines.	Disable the following algorithms: • Top Countries • Internet Threats Monitor • DDOS Violations • Nefarious activity
When initially evaluating SonicWALL Scrutinizer the interface is slow and many interfaces don't immediately appear.	If installing Scrutinizer on a machine that is already receiving flows from > 50 devices, Scrutinizer will need an extra 5 minutes to crunch the data and display all that it is receiving.
The interface of SonicWALL Scrutinizer is very sluggish and / or the collector may fail and need to be restarted.	The performance of Scrutinizer is dependent on processing power of the machine it is installed on. NOTES: • VMware is often not a good platform • SAN storage can be slow • Turn Anti-virus off or exclude the Scrutinizer directory
Multiple CPUs mislabeled in Vitals Summary	Fix coming in a future release.
Loading a single report in Scrutinizer consumes roughly 90MB-95MB of memory.	Solution being considered. Possibly addressed in future release. Currently functioning as designed.
Issues displaying SonicWALL Scrutinizer in Internet Explorer v6	Internet Explorer v6 is no longer supported. Please use Internet Explorer v7 or newer. The latest version of any browser is highly recommended.
Bad formatting in report type when no data is available.	Fix coming in a future release.
Pie Charts error with "Graphing Error: No data for selected period" when results are zero.	Fix coming in a future release.

Resolved Issues

This section contains a list of resolved issues in the 9.0.1 release.

Symptom	Condition
Logalot creates empty and extra tables that are not used.	Occurs when using the Logalot feature.
“scrut_util” does not verify proper permission.	Occurs when running “scrut_util” from the command line interface.
Logalot Report Manager button does not work in the Admin tab.	Occurs when navigating to the **Admin** tab and clicking the **Logalot Report Manager** button.
Users cannot run Exceeded Crosscheck Fault Index as a report.	Occurs when trying to run Exceeded Crosscheck Fault Index as a report.
Removing a report policy does not properly remove scheduled reports.	Occurs when removing a report policy. The scheduled reports should be removed when the report policy is deleted.
SNMPv3 credentials cannot be set as the default credentials.	Occurs when configuring administrator’s credentials.
An error displays in the command line interface.	Occurs when running “scrut_util -update_plixerini_mysqlroot” in the command line interface.
Confusion with the naming convention of Custom Reports.	Occurs when viewing or configuring Custom Reports. To avoid confusion, Custom Reports are now called Flow Reports.
Threats Overview and FA, list alarms user shouldn't access.	Occurs when viewing the Alarms list in Threats Overview and FA.
There are some usability issues with the top interface gadget.	Occurs when searching for addresses in the top interface gadget.
The Reset Hits button does not reset all counts.	Occurs when navigating to the **Policy Manager** page and clicking the **Reset Hits** button.
Column and sorting issues in the Bulletin Board.	Occurs when navigating to the Bulletin Board.
Some upgrades would cause the installer to become unresponsive before a file copies.	Occurs when installing an upgrade for the Scrutinizer feature.
Some issues excluding Violators in the Alarms > Advanced Filtering page.	Occurs when navigating to the **Alarms** tab, clicking the **Advanced Filters** button, and then excluding **Violators**.
Some minor grammar and formatting issues are displayed in the Scrutinizer management interface.	Occurs when viewing the Scrutinizer management interface.
Some users may have removed Listening Port 4739.	Occurs when removing Listening Port 4739. The FlowAlyzer needs this port to function properly.
Users sometimes get 0 results after Flow View is deployed.	Occurs when launching Flow View for some alarms.
The date selector may vanish.	Occurs after running a multiple Logalot graph report
Logalot debug settings do not properly hide after the Debug menu is disabled.	Occurs when disabling the Debug menu.

Symptom	Condition
Users can use decimal places when ordering policies.	Occurs when ordering policies.
The installer displays an error message informing the user that it cannot overwrite “scrut_util.exe.”	Occurs when using the Scrutinizer installer.
The Scrutinizer system may restart prematurely during an upgrade.	Occurs when performing a Scrutinizer update. In 9.0.1, services will be disabled during upgrades to prevent restart prematurely.
The link to online help is broken in the Dashboard tab.	Occurs when clicking the **Online Help** in the **Dashboard** tab.
The link to the Alarms tab is not accessible from the top network transport gadget.	Occurs when clicking the Alarms tab in the top network transport gadget.
The Enter key does not perform a search, only the Search button works.	Occurs when navigating to the **Alarms > Policy Manager** page, entering search criteria in the **Search** text-field, and then pressing the **Enter** key.
An error displays in the command line interface.	Occurs when running “scrut_util -update_httpd_port” in the command line interface.
The “statusAverage” server preference is no longer relevant.	The “statusAverage” server preference is removed in 9.0.1.
Some buttons do not have mouse over descriptions.	Occurs when navigating through the Scrutinizer management interface and moving the mouse over buttons to view a description.
Alarm reports for the Flowalyzer device display no results.	Occurs when configuring an alarm report on the Flowalyzer device.
Source and Destination Country Filter does not work.	Occurs when there are no destination countries.
Crosscheck and Service Level Reports are displayed incorrectly.	Occurs when SPM users are viewing the Crosscheck and Service Level reports.
Email notifications are not sent out.	Occurs when Email notifications are sent out for Rate Based triggers.
Launching dashboards can be slow.	Occurs when launching certain dashboards.
Device syslogs are being sent down from Flowalyzer.	Occurs when Flowalyzer sends down device syslogs.
No search results are listed for “Limited SPM Users.”	Occurs when using the Top Interface Gadget to search for “Limited SPM Users.”
A Packets column is incorrectly displayed in Outbound.	Occurs when viewing the Top Interfaces report.
Jitter reports are incorrectly showing available for some Medianet exporters.	Occurs when viewing the Jitter reports.
An incorrect status is showing up in Tree menu.	Occurs when viewing the Tree menu.

Symptom	Condition
The Watcher is becoming unresponsive at 1 AM.	Occurs when using SNMP in conjunction with the Watcher.
Flow Direction is exported with only ingress flows.	Occurs when exporting the Flow Directions feature.
Violation reports are inaccurate.	Occurs when the FIN algorithm does not report violations with the correct accuracy.
FA Top Hosts Gadget is not render properly with less than 10 hosts.	Occurs when using the FA Top Hosts Gadget with less than 10 hosts.
An inadequate message appears in server preferences, related to listening ports issues.	Occurs when viewing the server preferences.
The Alarm tab experiences delays.	Occurs when interrupting the column sorting process.
Device Details report egress for “sFlow” interfaces.	Occurs when navigating to **Device Details** and viewing the **Egress** for “**sFlow**” interfaces.
The Status tab constantly refreshes.	Occurs when navigating to the Status tab.
Some of the Country definitions are missing.	Occurs when viewing the **Policy Manager > Definitions** page.
The Top Conversations gadget does not resolve addresses via DNS.	Occurs when viewing the Top Conversations gadget.
Outbound interface reports do not show outbound results on the last 5 min reports.	Occurs when reports are run for the outbound interfaces.
The Crosscheck summary does not verify the subnet mask properly for custom networks	Occurs when viewing the Crosscheck summary.
Some vitals may have gaps.	Occurs when running the Vital function.
SonicWALL Spyware report filters do not work properly.	Occurs when running a SonicWALL Spyware report.
The Top Countries gadget links do not work properly.	Occurs when using the Top Countries gadget.
The Security > User Groups manageable gadgets are not in alphabetical order.	Occurs when viewing the **Security > User Groups** page.
The NULL Scan Violations in Flow View may cause an error.	Occurs when using Null Scan Violations.
The user may see a timeout message related to server preferences.	Occurs when saving from server preferences.
Service Provider users might have unwanted access to Service Level reports.	Occurs when accessing the Service Level reports.
Some FA Configuration graphs are missing historical trends.	Occurs when viewing the FA Configuration graphs.

How to Upgrade to the Licensed Version

Click the Scrutinizer link on the www.mysonicwall.com homepage to automatically register a Scrutinizer product with its own serial number. The user is then directed to the Services Management page for the newly registered Scrutinizer product. Upon registration, SonicWALL Scrutinizer will be available from the Downloads section in mySonicWALL.

The free trial version of Scrutinizer can be installed immediately and does not require a license key; just double click the executable and follow the installation process.

The new Scrutinizer product will be listed in the My Products section on mySonicWALL. Click on the Scrutinizer product to bring up the Services Management page for that particular product.

Additional software modules and support licenses can be activated on the Services Management page either by clicking on the Buy Now button or by either entering the appropriate keys purchased from a SonicWALL reseller or distributor.

Upon activation of any additional licenses, an email with instructions on how to download a license file will be sent to the email address associated with the mySonicWALL account. The license file will be available in the My Downloads section of the Download Center of MySonicWALL.

Once a license file is obtained, bring up the SonicWALL Scrutinizer web interface, i.e. the Scrutinizer application itself, and click on the Admin tab. In the left navigation bar, click **Settings > Licensing**. Paste the license key into the appropriate box. Click the **Save** button.

.

FAQ

What is NetFlow?

Cisco® NetFlow technology is an embedded feature within Cisco IOS routers and high end switches (e.g. 6500 series). NetFlow data records consist of information about source and destination addresses, along with the protocols and ports used in the end-to-end conversation. Scrutinizer uses this information to generate graphs and reports on traffic patterns and bandwidth utilization. More information can be found here.

What is sFlow?

Unlike NetFlow which aggregates multiple conversation streams into a single packet, sFlow is a packet sample of traffic. Although it offers 100% of the packet, when used strictly for IP accounting, it is unreliable.

What are the different versions of NetFlow available?

Version 1 is the original format supported in the initial NetFlow releases, while version 5 is the standard and most common NetFlow version deployed. Version 5 is an enhancement that adds Border Gateway Protocol (BGP) autonomous system information and flow sequence numbers. Version 6 is similar to version 7. This version is not used in the new IOS releases. Version 7 is an enhancement that exclusively supports NetFlow with Cisco Catalyst 5000, 6500 and 7600 series switches. Version 8 is an enhancement that adds router-based aggregation schemes. It was introduced to reduce resource usage, and includes a choice of eleven aggregation schemes. Version 9 is an enhancement to support different technologies such as Multicast, Internet Protocol Security (IPSec), and Multi Protocol Label Switching (MPLS). Versions 2, 3 and 4 either were not released.

Scrutinizer currently supports:

- NetFlow versions 1,5,6,7 and 9
- sFlow version 2, 4 and 5
- Flexible NetFlow, IPFIX, JFlow and NetStream.

How is NetFlow different from traffic analyzers like MRTG?

MRTG and other such equivalent tools provide information that is largely limited to SNMP statistics. NetFlow is more geared toward application-level details such as hosts, protocols, and conversations, which are an inherent part of IP traffic.

Is Cisco the only vendor supporting NetFlow?

NetFlow technology was invented by Cisco, and Cisco IOS devices offer NetFlow compatibility. There may be other vendors offering NetFlow support on their devices. Scrutinizer has been tested on over a dozen different vendors.

Is a trial version of Scrutinizer available for evaluation?

Yes. A free version of Scrutinizer can be downloaded and you can get an evaluation license to try the full version.

What are the differences between the free and commercial version?

The commercial version of Scrutinizer NetFlow & sFlow Analyzer includes the Flow Analytics add-on module, which adds historical data retention and network behavior analysis.

What are the system requirements?

Scrutinizer's system requirements are detailed here: System Requirements

How do I find out if my Cisco equipment supports NetFlow?

Review the NetFlow Services Solutions Guide to find out if you have a NetFlow compatible Cisco router or switch.

What if I need features that Scrutinizer does not support?

We understand that our software needs to be flexible. If you want a feature added, we may be able to work with you.

Does it support other Languages?

Scrutinizer currently supports the following languages; Chinese (Simplified and Traditional), English, French, German, Japanese, Korean, Portuguese, Russian, and Spanish.

How will enabling NetFlow affect the performance of the router/switch?

For detailed information on exactly how enabling NetFlow will affect the performance of your Cisco router or switch, review the NetFlow Performance Analysis whitepaper [PDF]: http://www.cisco.com/en/US/technologies/tk543/tk812/technologies_white_paper0900aecd802a0eb9.html.

How long do I have to wait before the graphs are populated?

Less than 5 minutes. Make sure you have the NetFlow configured correctly on the router or switch.

Why are some interfaces labeled as IfIndex2, IfIndex3 or just 1, 2, 3, etc.?

This happens if the interfaces did not respond to the SNMP requests sent by Scrutinizer. Bring up the SNMP view that lists all the interfaces and click the Update button. Please review SNMP Device View in the Scrutinizer manual.

Also, this will occur if flow option templates to identify the interfaces have not been received.

How do I enter IP to name resolutions so that Scrutinizer doesn't have to use the DNS to resolve IPs?

Edit this file: C:\WINDOWS\system32\drivers\etc\hosts and enter the IP to name translations.

Overall utilization on the interface appears to be understated. Why would this be?

1. Make sure NetFlow is enabled on all physical interfaces of the device. Do not be concerned with the virtual interfaces, as they will auto-appear once NetFlow is enabled on the physical interface.
2. If the hardware can't keep up with sending the NetFlow packets, it will drop NetFlows before they even leave the device. To check to see if this is the problem, login to the Cisco device.
   Command to type: Router_name>**sh ip flow export**

   At the bottom of the export, look for something like "294503 export packets were dropped due to IPC rate limiting". If this counter is incrementing, the hardware cannot keep up with the export demands.
3. The command below breaks up long-lived flows into 1-minute segments. You can choose any number of minutes between 1 and 60; if you leave the default of 30 minutes you will get spikes in your utilization reports. Command to type**: ip flow-cache timeout active 1**
4. The command below ensures that flows that have finished are exported in a timely manner. The default is 15 seconds; you can choose any value between 10 and 600. Note however that if you choose a value that is longer than 250 seconds Scrutinizer may report traffic levels that appear low.
   Command to type: **ip flow-cache timeout inactive 15**

   NetFlow only exports IP traffic (i.e. no IPX, etc.) and no layer 2 broadcasts are exported by this version of NetFlow.

How do I setup my router to forward NetFlows to two destinations?

Type the "ip flow-export destination" command twice:

- router-name# **ip flow-export destination 10.1.1.8 2055**
- router-name# **ip flow-export destination 10.1.1.9 2055**

Why are my graphs reporting over 100% utilization?

1. The interface speed is not correct. Scrutinizer uses the speed specified in the SNMP OID. Login to the router or switch and fix the problem or in Scrutinizer go to Device Details and manually type in the correct speed.
2. The active timeout has not been set to 1 minute on the router. Login to the router or switch and fix the problem.
3. Non-dedicated burstable bandwidth, where the ISP allows you to use over the allocated bandwidth.
4. Both ingress and egress NetFlow collection have been enabled on the interface. This can work properly if the direction bit is set in the egress flows. Scrutinizer works ideal when only ingress NetFlow collection is configured on all interfaces. Only egress on all interfaces is also possible.
5. Do you have any encrypted tunnels on the interface?
   - ◦47 - GRE, General Routing Encapsulation.
   - ◦50 - ESP, Encapsulating Security Payload.
   - ◦94 - IP-within-IP Encapsulation Protocol.
   - ◦97 - EtherIP.
   - ◦98 - Encapsulation Header.
   - ◦99 - Any private encryption scheme.

   This can cause traffic to be counted twice on an interface. In Scrutinizer, go to Admin Tab > Definitions > Manage Exporters. Click on the round icon with the '-'. When you mouse over the icon, the ALT will display "View the current protocol exclusions of this device." Click on this and make sure the above protocols are being excluded.

6. Full Flow Cache: All flows are stored in the flow cache on the router before export. Once the cache is full, it stops adding entries into the cache until it expires them. When events such as a DDOS or a "social event" occur, the router's cache becomes full. The cache can be increased; however, it will use more memory and could have a negative impact on the router. A loss of flows will cause Scrutinizer to understate utilization.

How do I find out if any updates are available for Scrutinizer?

In your local Scrutinizer install, click the Status tab. If updates are available, you will see a spinning blue icon in the upper right hand corner. If you have a proxy server, this spinning icon will always appear. Click on it to find out the latest version.

Users can also use the **-v** parameter for any **\scrutinizer\cgi-bin*.cgi** or **\scrutinizer\bin*.exe** file to get the current version and build for that executable.

Example: **scrut_util -v**

Compare this to the Scrutinizer Update History.

I have forgotten my Scrutinizer password. How do I find out what it is?

In your local Scrutinizer install, type the following commands in a command prompt, from the [homedir]\bin\ directory:

scrut_util.exe -reset_admin_password [USERNAME]

The USERNAME is the name of the Scrutinizer user account to modify. When the command is executed, it will prompt for the new password, and then to re-enter it.

Note: These commands must be run from the Scrutinizer server.

How do I setup SSL with Scrutinizer?

An installer with SSL support is available for eligible parties. Please contact us for the SSL installer.

How do I use a different drive for storing data?

Note: The following procedures will not work for remote drives based on Windows shares.

1. Stop the plixer_mysql service.
2. Copy the **[homedir]\Scrutinizer\mysql\data** directory to the new drive.
3. Edit the **[homedir]\Scrutinizer\mysql\my.ini** file, changing the drive letter for the **datadir=x:[homedir]/SCRUTINIZER/mysql/data/** entry.
4. Start the **plixer_mysql** service.

For more information on using a different drive for stored data or storing data to a remote database with Scrutinizer version 7 or higher, review this guide.

Why do not all of the colors print correctly when I try to print an emailed report?

This can be caused by an option found in some browsers and email clients.
In Internet Explorer:

1. Open the "Tools" menu.
2. Click "Internet Options.
3. Click the "Advanced" tab.
4. Scroll down to the "Printing" section.
5. Check "Print background colors and images.
6. Click "OK."

This change will carry over to Outlook and Outloook Express.

Can Scrutinizer run in VMWare?

Yes, but as with any virtualized environment, you may experience sharp declines in performance when your server's resources are divided between many sessions.

How do I exclude Scrutinizer in Symantec AntiVirus?

1. From within Symantec, expand the "Configure" option from the tree menu and select "File System."
2. Click the "Exclusions" button.
3. Click the "Files/Folders" button.
4. Find the Scrutinizer directory and check the box next to it.
5. Click "OK" to finish.

How do I setup integration between Scrutinizer and WhatsUp Gold?

Visit the WhatsUp Gold Integration page for instructions on setting up WhatsUp Gold v12/v14 and Scrutinizer to work together.

Why are my IPs not resolving, even though I have configured my DNS properly in Windows?

In certain situations, Scrutinizer may not be able to properly resolve IP addresses. This usually happens when there are multiple DNS servers with disparate records. To deal with this, Scrutinizer allows you to specify your DNS servers in a file rather than get the settings from the Windows Registry. The steps are outlined below:

1. Create a file in the **\scrutinizer\html** directory called **dns.conf**.
2. Open this file with a text editor like Notepad.
3. Create a list of DNS servers in the file in the format below.
   - nameserver 192.168.1.1
   - nameserver 166.186.184.2
   - nameserver 224.39.1.171

   Now that you have created this file, you should now be able to go into the Scrutinizer web interface and do lookups properly.

I'd like to change the MySQL "scrutinizer" user password from the default to something more secure. Is there anything else I need to do other than set the password in MySQL?

Update MySQL Root password via CLI using **scrut_util.exe** located in the **[HOMEDIR]\Scrutinizer\bin** directory. There is a two-step process, resetting the password then updating the **plixer.ini** file.

Options:
-**reset_mysql_password**
Changes the MySQL root account password.
-**update_plixerini_mysqlroot**

Use this command to update the **plixer.ini** database root user password. Scrutinizer and the database root password must be in sync.

Usage Example:
C:\Program Files (x86)\Scrutinizer\bin>scrut_util.exe -reset_mysql_password
Changing Password for MySQL Root Password. Press <ENTER> to abort.

Note: On Windows 2008 and Windows 7, you must run this command from the Administrator Dos Prompt

New Password:
Verify Password:
Attempting to login with new password ... PASS!
Password Updated for MySQL Root ... DONE!

Where can I find the Scrutinizer manual?

A copy of the Scrutinizer manual is included with your product. Just click any of the "?" icons.

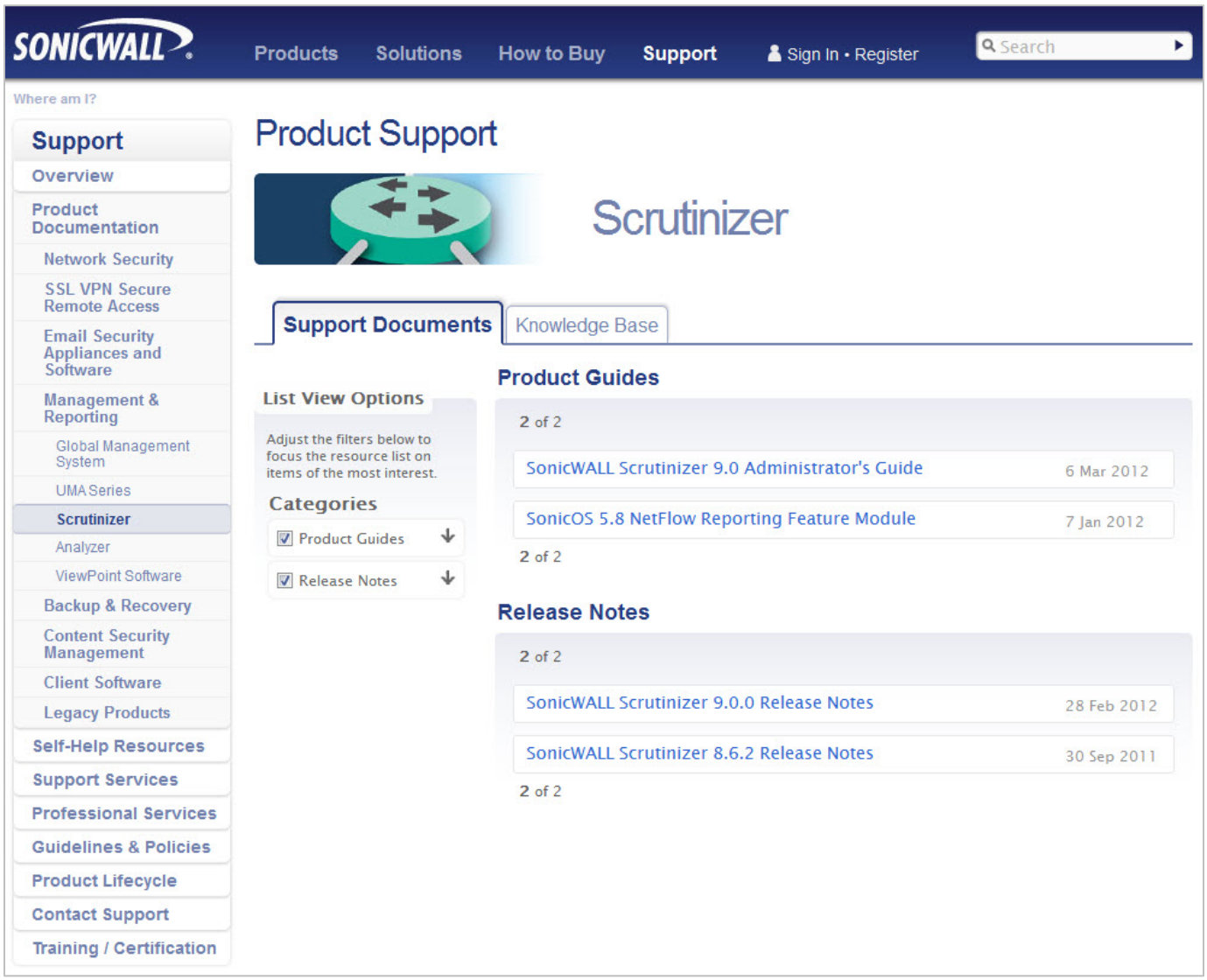
How do I know how much hard drive space I will need?

Use the NetFlow Bandwidth and Hard Drive Consumption Calculator to determine how much hard drive space your NetFlow data will consume.

Related Technical Documentation

SonicWALL Scrutinizer reference documentation is available at the SonicWALL Technical Documentation Online Library: http://www.sonicwall.com/us/support/6632.html

More information on NetFlow Services is available on the SonicWALL Web site.



Last updated: 4/25/2012