



STEALTHWATCH® FLOWSENSOR™

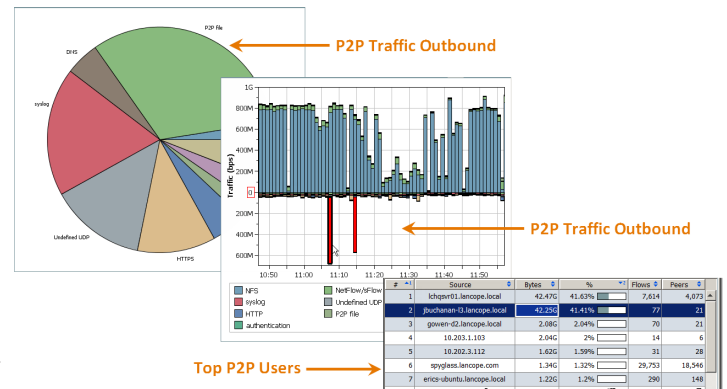
In today's complex business environments, organizations demand continuous access to and fast performance from the business-critical applications they use. When these fail or slow down, network operations and security teams must be able to isolate the root cause and restore performance in both physical and virtual environments quickly and efficiently.

Complicating matters is the fact that with the advent of Web 2.0, as much as 85% of all network traffic now goes through port 80. As a result, distinguishing between individual applications has become increasingly difficult. To optimize performance and secure the network, both network operations and security teams need to know what, when and how applications are in use — and by whom — across the enterprise.

Reliably Identify True Layer 7 Application and Protocol Information with DPI and Behavioral Analytics

The StealthWatch FlowSensor from Lancope®, the leader in flow collection and analysis, uses a combination of deep packet inspection (DPI) and behavioral analysis to identify applications and protocols in use across the network — no matter if they are plain text or use advanced encryption and obfuscation techniques.

Providing true Layer 7 application visibility, the FlowSensor gathers application information and URL data, along with packet-level performance statistics. With unmatched scalability, the FlowSensor provides the all-encompassing visibility needed anywhere from branch offices to 10G data centers at a fraction of the cost of traditional probe-based devices.



The StealthWatch FlowSensor provides valuable insight into application activity, such as P2P traffic. When coupled with other StealthWatch System components, managers can see how much of their overall traffic is comprised of P2P. Drilling deeper, operators can see when this activity took place and which users were involved.

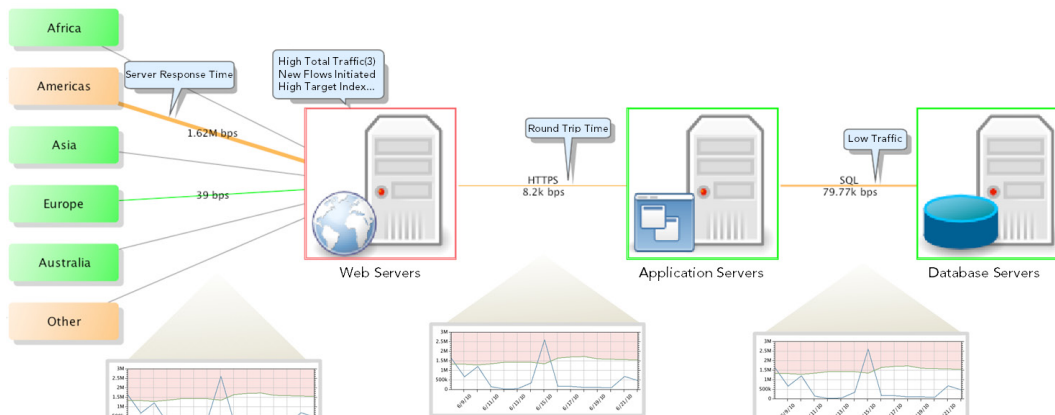
The FlowSensor recognizes more than 900 application variants and their classifications, such as¹:

- ▶ Peer-to-Peer (e.g., BitTorrent, eDonkey and Kazaa)
- ▶ Business-critical (e.g., Exchange, LDAP and SAP)
- ▶ Social media (e.g., Facebook, MySpace and LinkedIn)
- ▶ Streaming audio and video (e.g., YouTube and Pandora)
- ▶ Instant Messaging (e.g., Jabber and MSN)
- ▶ Voice over IP (e.g., Skype, H.323 and SIP)
- ▶ Mobile (e.g., Blackberry)
- ▶ Tunneling (e.g., SSL, IPsec, L2TP and GRE)
- ▶ Standard applications (e.g., HTTP and DNS)
- ▶ Gaming (e.g., World of Warcraft and Xbox)

¹ For a complete list, see the [StealthWatch FlowSensor Supported Applications Data Sheet](#).

Diagnose Performance Issues: Application vs. Network vs. Security

Without knowing what is typical for application and network performance in physical and virtual environments, network and security teams cannot proactively determine when latency is a problem. The FlowSensor gathers packet-level performance statistics, which StealthWatch analyzes to build a baseline of application and network performance. If performance degradation occurs, StealthWatch automatically alerts operators and helps isolate the root cause within seconds to a specific application, network or security issue.



As an integral part of the StealthWatch System, the FlowSensor provides operators with the contextual intelligence necessary to resolve performance issues quickly and easily.

In addition, network attacks, viruses, worms and other malware can also impact application performance. StealthWatch zooms in on any unusual behavior and immediately sends an alarm with the contextual intelligence that allows security personnel to take quick, decisive action to mitigate any damage.

If the cause lies with a particular host, StealthWatch can even identify the user involved. Using StealthWatch’s unique drill-down features, operators can go from identifying the issue to isolating the root cause within seconds, thereby reducing Mean-Time-To-Know (MTTK), enhancing operational efficiency and reducing costs.

Advanced URL Data

Lancope also provides URL information in flow records generated by the FlowSensor. Previously unavailable from most flow sources, URL data enables administrators to see exactly which web sites users are going to, as well as the file path, to more easily identify which applications are causing performance or security problems. Administrators can identify both the hostname of the server, as well as any error messages within the flow, for faster network troubleshooting.

Client Host	Client Host Groups	Client Application Det...	Server Host	Server Host Groups	RTT...	SRT...
10.201.10.100	Desktops, VLAN201, Los Angeles	GET http://na3.salesforce.com/00Q5000000ZSz11	204.14.29.200	Salesforce, United States	19ms	2086ms
10.201.10.100	Desktops, VLAN201, Los Angeles	GET http://www.salesforce.com/	204.14.29.200	Salesforce, United States	18ms	85ms

URL data from StealthWatch helps further distinguish which applications are causing security or performance problems.

Complete, Scalable Packet-Level Visibility from Branch Offices to 10G Data Centers

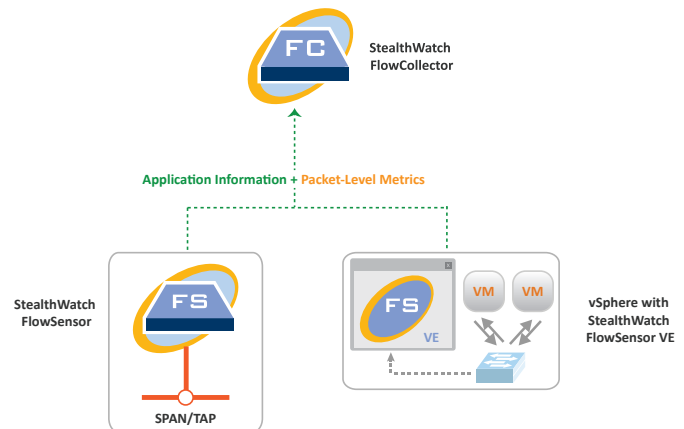
The FlowSensor is available either as a lightweight 1U appliance or as a virtual image. The available appliances include the compact form-factor FlowSensor 250, which offers a throughput of 100 Mbps for lower bandwidth areas of the network, and scale up to the FlowSensor 3000 for monitoring 10G networks.

For virtual environments with limited system resources, the FlowSensor VE (Virtual Edition) enables operators to see the same detailed traffic statistics for their virtual networks as they can see for their physical networks, effectively eliminating the blind spots often associated with virtualized environments.

How It Works

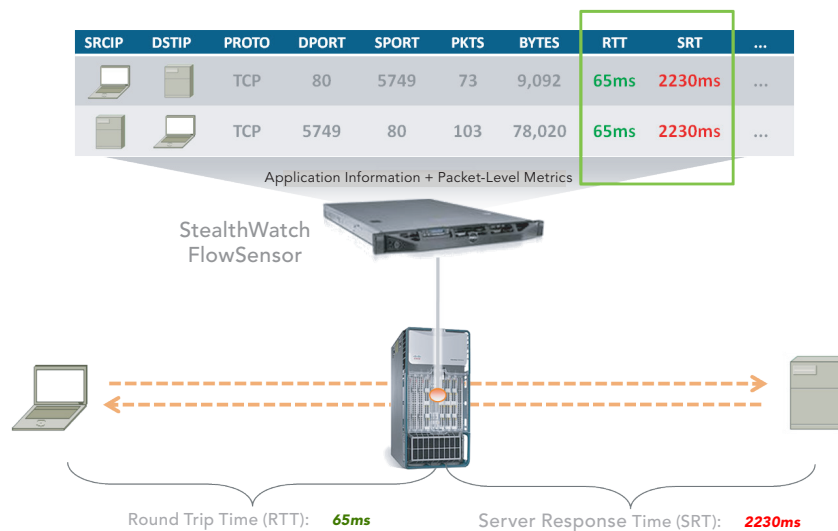
The FlowSensor physical appliance easily connects into existing infrastructure via a SPAN, mirror port or Ethernet TAP. The FlowSensor VE is a lightweight image that simply installs inside each vSphere/ESXi host and connects promiscuously to the virtual switches.

Once installed, the FlowSensor passively captures Ethernet frames from the traffic it observes and gathers packet-level data containing valuable session statistics that pertain to conversational pairs, bit rates and packet rates. As the FlowSensor observes network traffic, it also calculates various performance statistics for each flow and exports them — enriched with performance metrics and behavioral indicators — to the StealthWatch FlowCollector.

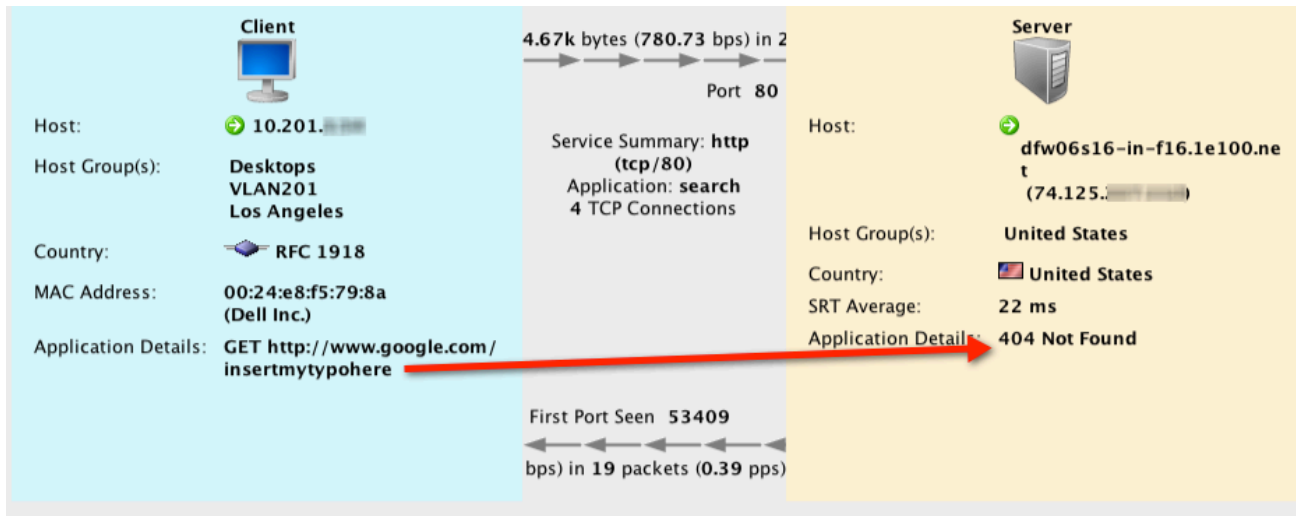


The StealthWatch FlowSensor connects easily into existing infrastructure to deliver application information, URL data and packet-level performance metrics.

Because the FlowSensor has packet-level visibility, it can calculate performance metrics, such as round-trip time (RTT), server response time (SRT) and packet loss for TCP sessions. It includes all of these additional fields in the records that it sends to the StealthWatch FlowCollector. These flow performance indicators provide insight into the latency introduced by the network, as well as by the server-side application.



Performance metrics, such as round-trip time and server response time, are immediately apparent through the StealthWatch FlowSensor's packet-level visibility.



With advanced URL data, administrators can also view any error messages within the flow to further expedite network performance troubleshooting.

The FlowSensor Helps Organizations:

- ▶ **Use deep packet inspection to identify Layer 7 applications** traveling across both physical and virtual environments
- ▶ **Identify encrypted and obfuscated applications** and protocols by packet-level behavioral analysis
- ▶ **Gather packet-level performance statistics** for all IP traffic traveling across the network
- ▶ **Troubleshoot application performance and network latency issues** through quick diagnosis and resolution of end-user performance complaints
- ▶ **Achieve comprehensive visibility** into areas of the network that lack flow data or where traditional probe technology is too costly to deploy
- ▶ **Monitor network communications** down to the individual flow by gathering communications information across the network, delivering unmatched visibility into the nature of the organization's network traffic
- ▶ **Pinpoint security-related performance problems** by gathering the packet-level data that StealthWatch analyzes to identify and prioritize suspicious network communications, including botnets, worms, policy violations and misconfigured network devices on the network that lack flow data or where traditional probe technology is too costly to deploy
- ▶ **View advanced URL data** to further expedite troubleshooting

To learn more or request a demo, contact sales@lancope.com.



FlowSensor Appliance Specifications

	FS 250	FS 1000	FS 2000	FS 3000
Communications				
Throughput	100 Mbps	1.0 Gbps	2.5 Gbps	5.0 Gbps
Interfaces				
Management Port	1 Cu; 10/100/1000			
Monitor Port	2 Cu; 10/100/1000	3 Cu; 10/100/1000	5 Cu or 3 Cu and 2 optical fiber; 10/100/1000	2 optical fiber; 10 GB (Intel PRO 10GBE SR-XFP)
Console Port	Serial	Serial, KVM *		
Physical				
Form Factor	1U-Short Rack (Stackable)		1U Rack (Stackable)	
Height	4.5 cm (1.75 in.)	4.24 cm (1.67 in.)	4.26 cm (1.68 in.)	
Width	43 cm (16.93 in.)	43.4 cm (17.09 in.)	With rack latches: 48.24 cm (18.99 in) Without rack latches: 42.4 cm (16.69 in)	
Depth	27.5 cm (10.83 in.)	39.37 cm (15.5 in.)	With power supplies and bezel: 77.2 cm (30.92 in) Without power supplies and bezel: 73.73 cm (29.02 in.)	
Weight	6 kg (13.23 lbs)	8.058 kg (17.77 lbs)	17.69 kg (39 lbs) maximum configuration	
Rails	Mounting ears	Rack chassis with Versa rail; round holes for third-party racks	Sliding Ready Rails with Cable Management Arm	
Storage	160 GB non-redundant		146 GB RAID-1	
Environmental				
Power	Single; 100 W	Single; 250 W	Redundant; hot-swappable; 717 W	
Heat Dissipation	341 BTUs per hour	1039 BTUs per hour	2446.5 BTU per hour maximum	
Temperature	Operating: 0° to 55° C (32° to 131° F) Storage: -20° to 70° C (-4° to 158° F)	Operating: 10° to 35° C (50° to 95° F) Storage: -40° to 65° C (-40° to 149° F)	Operating: 10° to 35° C (50° to 95° F) with a maximum gradation of 10° C (50° F) per hour Note: For altitudes above 2,950 feet, the maximum operating temperature is derated -17° C (1° F) per 550 feet Storage: -40° to 65° C (-40° to 149° F) with a maximum gradation of 20° C (68° F) per hour	
Relative Humidity	Operating: 5% to 95% (non-condensing) Storage: 5% to 95% (non-condensing)	Operating: 20% to 80% (non-condensing) with maximum gradation of 10% per hour Storage: 5% to 95% (non-condensing)		
Regulatory Compliance				
Please call for a complete list	<ul style="list-style-type: none"> • CE Emission • FCC Class A • RoHS 			

*Supports direct keyboard and monitor for configuration.

FlowSensor VE Specifications

Minimum Disk Space Requirements	VMware ESXi Versions Supported	Minimum Memory Requirements	Minimum CPU Requirements
1.4 GB	3.5 and 4.0	512 MB	2 GHz

About Lancope, Inc.

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales

+1.770.225.6500
888.419.1462

International Sales

+44 (0)560 344 8075

Website: www.lancope.com

E-mail: sales@lancope.com

©2012 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners.

DSV1002222012