Lancope®

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.

> "... uses a combination of **deep packet inspection (DPI)** and **behavioral analysis** to **identify** applications and protocols in use **across the network**..."

The StealthWatch FlowSensor Helps Organizations:

- Use deep packet inspection to identify Layer 7 applications
- Identify encrypted and obfuscated applications and protocols
- Gather packet-level performance statistics
- Troubleshoot application performance and network latency issues
- Achieve comprehensive visibility
- Manage network communications
- Pinpoint security-related performance problems

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

The StealthWatch FlowSensor from Lancope, a leader in network visibility and security intelligence, 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, along with packet-level performance statistics. With unmatched scalability, the FlowSensor provides the all-encompassing visibility needed anywhere from branch offices to 20G data centers at a fraction of the cost of traditional probe-based devices.

The FlowSensor recognizes more than 900 application variants and their classifications, such as[1]:

- Peer-to-Peer (e.g., BitTorrent, eDonkey and Kazaa)
- Business-critical (e.g., Exchange, LDAP and SAP)
- Social media (e.g., Facebook, Twitter 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., iPhone, Android)
- Tunneling (e.g., SSL, IPsec, L2TP and GRE)
- Standard applications (e.g., HTTP and DNS)
- Gaming (e.g., World of Warcraft and Xbox)

[1]Please contact sales for a complete list.

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 the StealthWatch System analyzes to build a baseline of application and network performance. If performance degradation occurs, the StealthWatch System automatically alerts operators and helps isolate the root cause within seconds to a specific application, network or security issue.

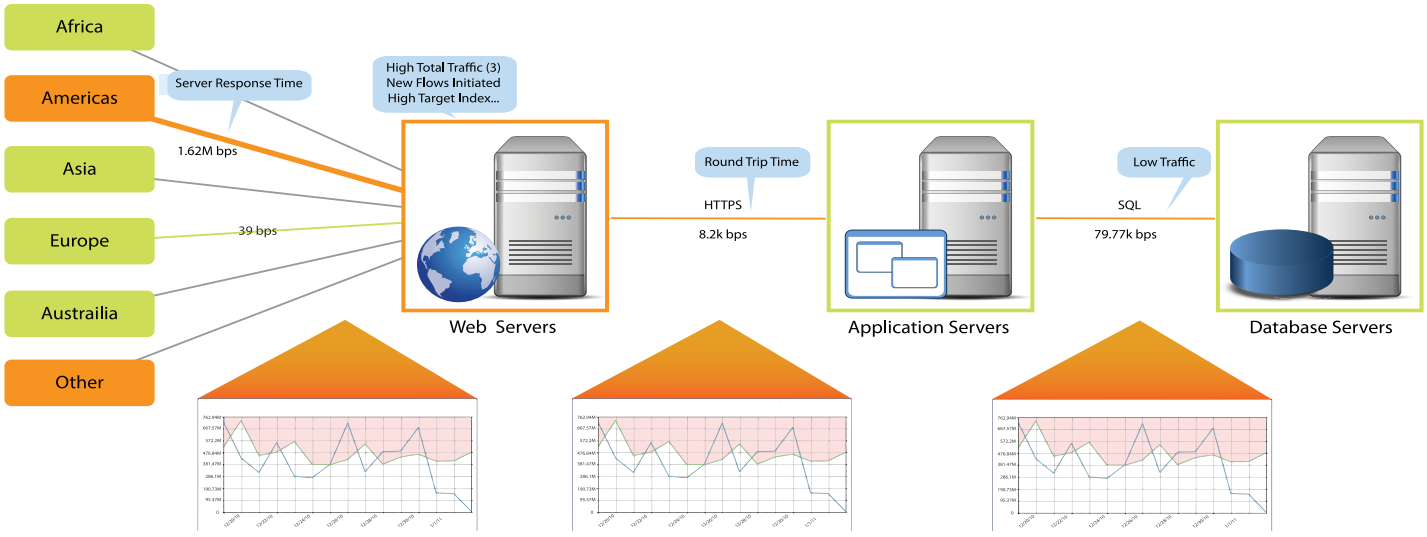
In addition, network attacks, viruses, worms and other malware can also impact application performance. The StealthWatch System zooms in on any unusual behavior and immediately sends an alarm with the contextual intelligence that allows security personnel to take quick, decisive action to mitigate any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

If the cause lies with a particular host, the StealthWatch System can even identify the user involved. Using the StealthWatch System'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.

Gain Complete, Scalable Packet-Level Visibility from Branch Offices to 20G 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 4000 for monitoring 20G 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.



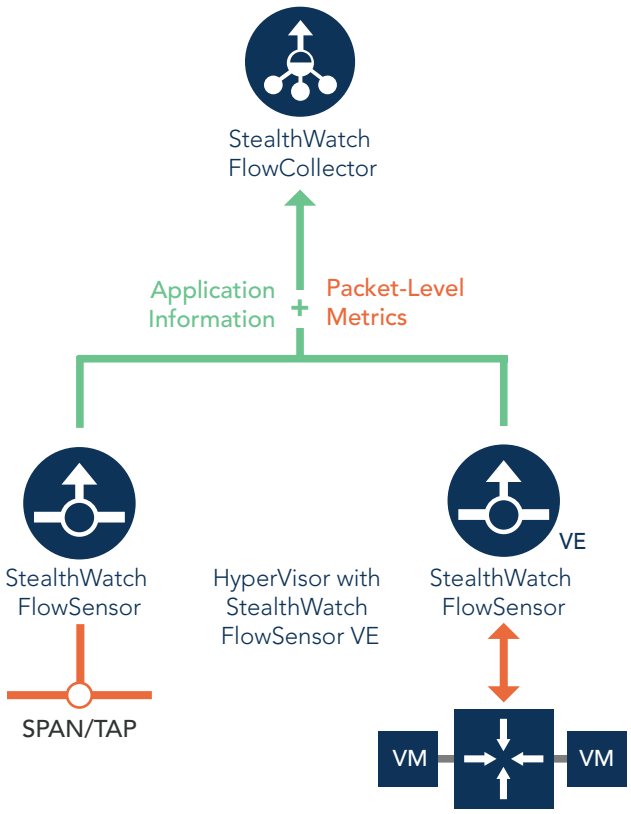
As an integral part of the StealthWatch System, the FlowSensor provides operators with the contextual intelligence necessary to resolve performance issues quickly and easily.

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.

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.



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

LEARN MORE. REQUEST A DEMO.

sales@lancope.com

FlowSensor Appliance Specifications

	FS 1010 *	FS 2010 *	FS 3010 *	FS 4010 *
Communications				
Throughput	1.0 Gbps (512 Byte Packets) 400 Mbps (64 Byte Packets)	2.5 Gbps (512 Byte Packets) 800 Mbps (64 Byte Packets)	5.0 Gbps (512 Byte Packets) 1.2 Gbps (64 Byte Packets)	20.0 Gbps (512 Byte Packets) 4 Gbps (64 Byte Packets)
Interfaces				
Management Port	1 Cu; 10/100/1000			
Monitor Port	3 Cu; 10/100/1000	5; 1 GB; 5 copper, or 3 copper and 2 fiber optic (Rated to monitor 2.5 Gbps)	2; 10 GB; fiber optic (Rated to monitor 5 Gbps total)	4; 10 GB; fiber optic (Rated to monitor 20 Gbps total)
Console Port	Serial, KVM **			
Physical				
Hardware Platform	R220	R630		
Hardware Generation	12G	13G		
Form Factor		Stackable		
Height	1.67 in (4.24 cm)	1.68 in (4.3 cm)		
Width	17.09 in (43.4 cm)	18.99 in (48.24 cm) With rack latches / 17.08 in (43.4 cm) Without rack latches		
Depth	15.5 (39.37 cm)	29.25 in (74.3 cm)		
Weight	35 lb (15.4 kg)	41 lbs (18.6 kg) maximum configuration		
Rails	1U-2 Post /4 Post Static Rails, Short	1U, Stackable Sliding Ready Rails		
Storage	500 GB Non-Redundant	300 GB (RAID-1 Redundant)		
Environmental				
Power	Single; 250 W (Nonredundant)	Redundant 750 W AC, 50/60 Hz; Auto Ranging (100V to 240V)		
Heat Dissipation	1040 BTUs per hour	2891 BTU per hour maximum		
Temperature	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: 10% 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	CE Emissions FCC Class A RoHS	• FCC (U.S only) Class A • DOC (Canada) Class A • VCCI Class A • UL 1950 • CSA 950 • CE Mark (EN 55022 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 60950)		

**StealthWatch System v6.7 specifications. **Supports direct keyboard and monitor for configuration.*

FlowSensor VE Specifications

Minimum Disk Space Requirements	Hypervisors Supported: VMware ESXi Citrix XenServer KVM	Minimum Memory Requirements	Minimum CPU Requirements
1.4 GB	v4.x or v5.x	512 MB	2 GHz