



STEALTHWATCH® MANAGEMENT CONSOLE

StealthWatch by Lancope is the leading solution for flow-based security and network performance monitoring across physical and virtual environments. With StealthWatch, network operations and security teams obtain actionable insight into who is using the network, what applications and services are in use and how well they are performing. StealthWatch delivers total, unified network visibility from a single, integrated platform by combining powerful network performance monitoring with deep packet inspection and behavior-based anomaly detection.

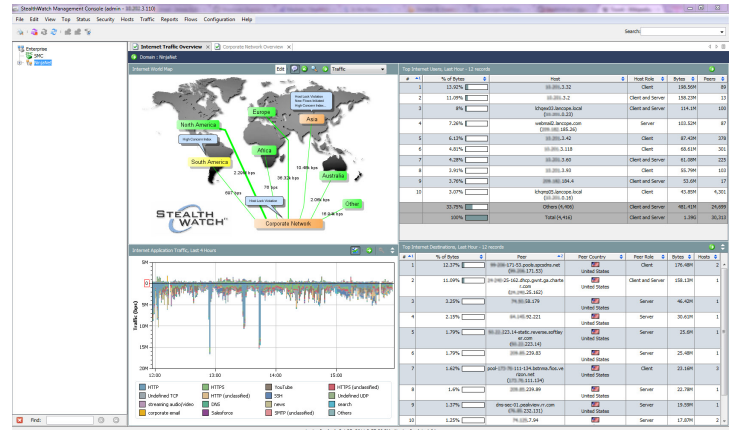
The StealthWatch Management Console (SMC) provides the single vantage point for disparate IT groups to see contextual information about all activity across the network and to investigate accordingly. It is available as either a physical or virtual appliance.

Solve Issues in Minutes, Not Days with End-to-End Visibility

With the SMC, gone are the days when different IT departments spent hours and even days trying to isolate the root cause of an issue – often blaming each other – before finally being able to deploy the appropriate personnel to take corrective action.

By simply glancing at the SMC's user-friendly graphical interface, operators can immediately spot and zoom in on any unusual behavior. Using the SMC's unique drill-down features, IT personnel can go from identifying the issue to isolating the root cause within minutes, identifying affected applications and users along the way, thereby reducing Mean Time To Know (MTTK), enhancing operational efficiency and decreasing costs.

Administrators can rapidly detect and prioritize security threats, pinpoint network misuse and suboptimal performance and manage event response across the enterprise – all from a single control center. Armed with graphical representations of network traffic, customized summary reports and integrated security and network intelligence, operators can easily identify internal and external attacks, network exposures and policy violations. The SMC also enhances network management through trend analysis, firewall and capacity planning, and performance monitoring.

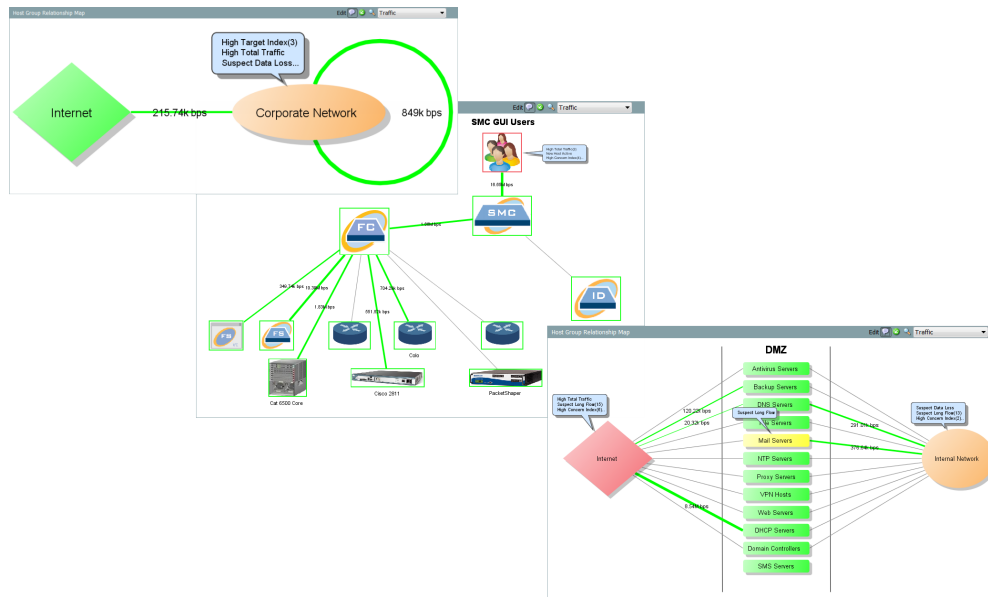


With customizable views and powerful drill-down capability, the SMC is the control center for network and security operations, performance management, traffic accounting, interface usage and user identity tracking.

Accelerate Problem Resolution with Customizable Relational Flow Mapping™

With real-time, customizable relational flow maps, the SMC provides network operations and security teams with graphical views of the current state of the organization's traffic. Within seconds, these teams can see exactly where to focus their attention.

The SMC allows administrators to easily construct maps of their network based on any criteria, such as location, function or virtual environment. By creating a connection between two groups of hosts, operators can quickly analyze the traffic traveling between them. Then, simply by selecting a data point in question, they can drill down to gain even deeper insight into what is happening at any point in time.



Relational flow maps enable network and security personnel to quickly identify areas that need attention.

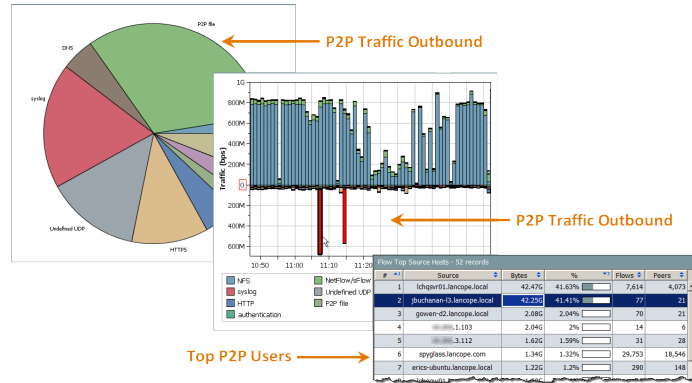
Quickly Break Volumes of Data Into More Meaningful Pieces with Advanced Reporting

As networks become more sophisticated and complex, the data required to monitor them becomes more and more voluminous. More data often means more time retrieving the pertinent information needed for troubleshooting and forensic analysis. Managers often want only a high-level overview of enterprise conditions without being overwhelmed with detailed data. Network operations and security teams can become frustrated while plodding through mountains of data to retrieve the specific detail they really need.

The SMC's advanced reporting mechanism meets both requirements by combining tremendous flexibility in the querying process with 1-minute granularity of flow data. This capability allows operators to run ad-hoc reports for arbitrary time frames, IP addresses and essentially any combination of criteria to access any data from high-level overviews down to specific flow details for any situation. Administrators can even schedule reports to run at specific times and set rules to email them automatically to the appropriate personnel.

Analyze Network Traffic Down to the Application and User Level

With the advent of Web 2.0, as much as 85% of all network traffic is now going through port 80. As a result, distinguishing between individual applications has become increasingly difficult. Both network operations and security teams need to know what, when and how applications are in use across the enterprise to optimize performance and secure the network.



Real-time visualization helps network and security teams understand traffic patterns, identify deviations from normal network behavior, pinpoint bottlenecks and spot malfunctioning devices, as well as detect DoS attacks, worms, reconnaissance and network misuse.

The SMC brings true Layer 7 application visibility to network and security teams by gathering application information and packet-level metrics and displaying them in easily understood pie charts, graphs and tables. In addition, administrators can use the SMC to define their own custom applications based on IP addresses. For example, one group of IP addresses can represent all of the Exchange servers in the organization. Another group of IP addresses can represent all of the DNS servers and so on.

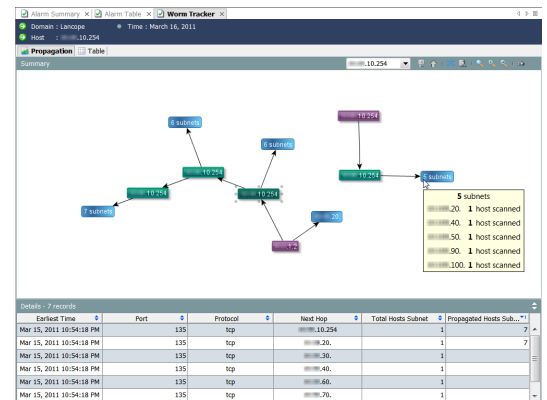
Visualize and Troubleshoot Worm Outbreaks and Other Attacks

The SMC empowers the security team to proactively identify threats on the network, such as when a new vulnerability is discovered targeting a service of a commonly used operating system. In addition, applications can carry viruses, worms and other malware that can impact network performance.

StealthWatch quickly zooms in on any unusual behavior, such as worm activity, immediately sending an alarm to the SMC with the contextual information necessary for security personnel to take quick, decisive action to mitigate any potential damage.

Control Who Sees What with the Right Point-of-View™

Authorized operators can access the SMC's user-friendly graphical interface from any local computer with a Web browser. StealthWatch's Point-of-View technology allows administrators to define different permission levels to ensure that only the appropriate personnel see information about certain segments of the network.



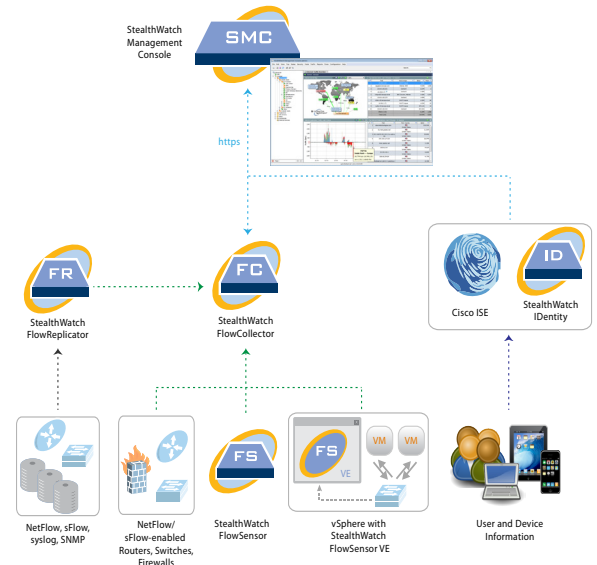
The SMC's sophisticated flow visualization enables operators to immediately understand worm activity, propagation and impact, quickly identifying points of entry to expedite incident response and fortify defenses.

How It Works

The SMC configures, coordinates and manages the StealthWatch System appliances, including FlowCollectors, FlowSensors and IDentity appliances. As these devices gather intelligence from critical segments throughout the enterprise, they feed it to the SMC. The SMC in turn correlates this information in real time and displays it in an easily understood graphical format.

Along with flow export technologies, StealthWatch can collect data from other types of technologies, such as firewalls, Web proxies, intrusion detection devices (IDSs), intrusion prevention systems (IPSs) and network admission control (NAC) systems. The SMC associates this data with behavior-based, flow-driven events, displays it graphically and stores it in the database for further analysis.

In addition, the flexible SOAP-compliant Web API provides ready programmable access to StealthWatch data from within enterprise applications, such as SIEMs, network managers, trouble-ticketing systems and third-party reporting systems.



The SMC provides centralized management, configuration and reporting for up to 25 StealthWatch FlowCollectors.

StealthWatch Management Console Features Matrix

Features	Network	Security
User identity tracking	✓	✓
Flexible deployment options, including virtual	✓	✓
Quick root-cause analysis, troubleshooting	✓	✓
Relational flow maps	✓	✓
Custom dashboards	✓	✓
Custom reports	✓	✓
Automated blocking, remediation or rate limiting	✓	✓
Top N reports for applications, services, ports, protocols, hosts, peers and conversations	✓	✓
Traffic composition breakdown	✓	✓
Customizable user interface based on Point-of-View	✓	✓
Support for multi-gigabit and large-scale MPLS network environments	✓	✓
Advanced flow visualization	✓	✓
Massive scalability	✓	✓
Combined internal and external monitoring	✓	✓
Capacity planning and historical traffic trending	✓	
WAN optimization reporting*	✓	
DSCP bandwidth utilization	✓	
Worm propagation visualization		✓
Internal security for high-speed networks		✓

*Limited functionality with sFlow

StealthWatch Management Console Specifications

	SMC 500 and 1000	SMC 2000
Network	Management Port — 10/100/1000 Copper	
Database Capacity	1 TB (RAID-5 Redundant)	2 TB (RAID-5 Redundant)
Rack Units (Mountable)	1U	2U
Power	Redundant 500W Auto Ranging (100V to ~240V)	Redundant 870W Auto Ranging (100V to ~240V)
Heat Dissipation	1,706 BTU per hour maximum	2,969 BTU per hour maximum
Dimensions	Height: 1.69 in. (4.3 cm) Width: 17.09 in. (43.4 cm) Depth: 24.69 in. (62.7 cm)	Height: 3.4 in. (8.64 cm) Width: 18.99 in. (48.24 cm) Depth: 28.4 in. (72.06 cm)
Weight	35.02 lb (15.9 kg)	57.54 lb (26.1 kg)
Rails	Sliding Ready Rails with Cable Management Arm	
Temperature	Operating: 50°F to 95°F (10°C to 35°C) with a maximum gradation of 50°F (10°C) per hour Note: For altitudes above 2,950 feet, the maximum operating temperature is derated 1°F per 550 feet. Storage: -40°F to 149°F (-40°C to 65°C) with a maximum gradation of 68°F (20°C) per hour	
Humidity	Operating Relative: 20% to 80% non-condensing with a maximum gradation of 10% per hour Storage Relative: 5% to 95% non-condensing	
Vibration	Operating Maximum: 0.26 Grms at 5-500 Hz for 15 minutes Storage Maximum: 1.54 Grms at 10-250 Hz for 15 minutes	Operating Maximum: 0.26 Gms at 5-350 Hz for 5 minutes Storage Maximum: 1.54 Gms at 10-250 Hz for 10 minutes
Shock	Operating Maximum: One shock pulse in the positive Z axis (one pulse on each side of the system) of 31G for 2.6 ms in the operational orientation Storage Maximum: Six consecutively executed shock pulses in the positive and negative X, Y and Z axes (one pulse on each side of the system) of 71G for up to 2 ms	Operating Maximum: Half sine shock in all operational orientations of 31G plus or minus 5% with a pulse duration of 2.6 ms plus or minus 10% Storage Maximum: Half sine shock on all six sides of 71G plus or minus 5% with a pulse duration of 2 ms plus or minus 10%; square wave shock on all six sides of 27G with a velocity change at 235 inches per second or greater
Altitude	Operating: -50 feet to 10,000 feet (-16 m to 3,048 m) Storage: -50 feet to 35,000 feet (-16 m to 10,600 m)	
Regulatory	<ul style="list-style-type: none"> • FCC (U.S. only) Class A • DOC (Canada) Class A • CE Mark (EN55022 Class A, EN55024, EN61000-3-2, EN 61000-3-3, EN60950) • VCCI Class A • UL 1950 • CSA 950 • EN 60950 <p>Please call for a complete list.</p>	

SMC Virtual Edition (VE)

The SMC Virtual Edition (VE) is designed to perform the same function as the appliance editions, but in a VMware environment. The following table shows the minimum resource requirements for the SMC VE to operate based on the number of FlowCollectors sending it data. However, the SMC VE scales dynamically based on the resources allocated to it. Therefore, for the SMC VE to operate effectively, be sure to allocate resources so that they are reserved for the SMC VE and not shared with any other virtual machines.

FlowCollectors	Concurrent Users	Reserved Memory	Reserved CPUs
1	Up to 2	4 GB	2
Up to 3	Up to 5	8 GB	3
Up to 5	Up to 10	16 GB	4

Note: For further details, see the StealthWatch System Capacities & Sizing Guidelines.

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.

DSV1602172012

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