



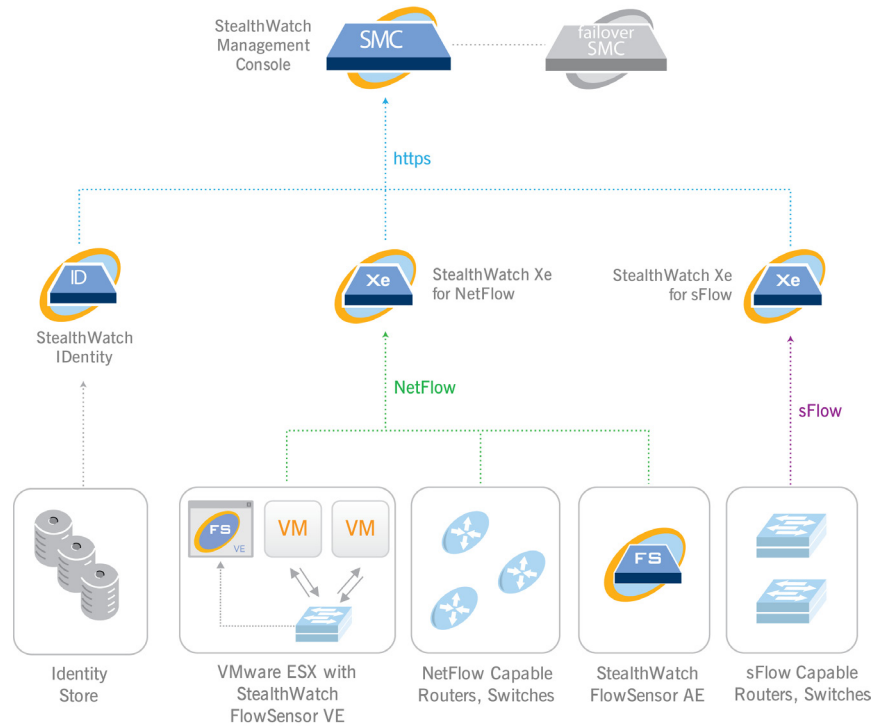
## STEALTHWATCH® MANAGEMENT CONSOLE

### Overview

The StealthWatch® Management Console (SMC) manages, coordinates and configures the StealthWatch System appliances, including StealthWatch Xe for NetFlow™ and sFlow® flow collectors, StealthWatch FlowSensor™ AE and VE and StealthWatch IDentity, to correlate security and network intelligence from critical segments throughout the enterprise. Delivering real-time insight into current network behavior, the SMC increases security and network team efficiency and decreases IT operations costs, while simultaneously improving overall security posture and operational awareness.

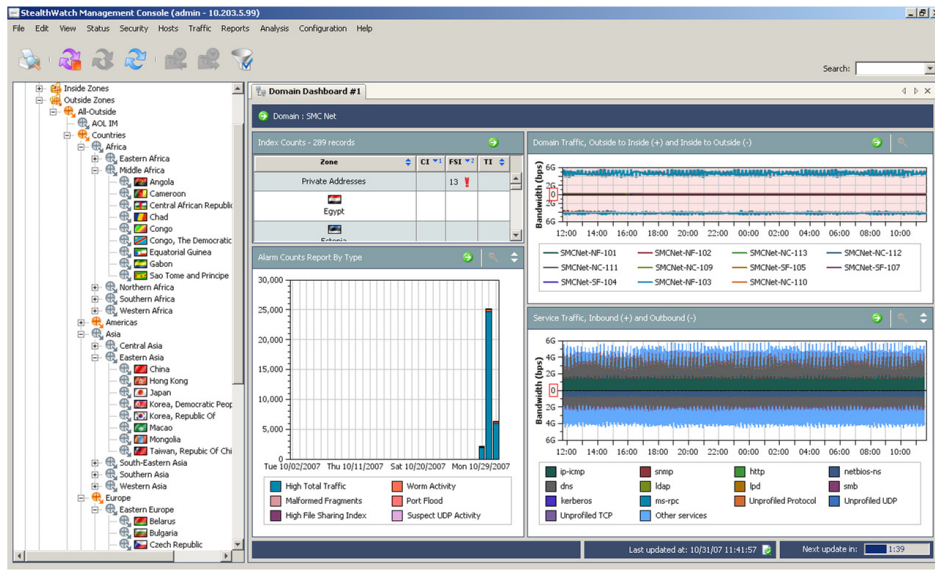
The SMC enables instant data correlation, traffic visualization and consolidated reporting. Administrators rapidly detect and prioritize security threats, pinpoint network misuse and suboptimal performance and manage incident response across the enterprise — all from a single control center.

Armed with graphical representations of network traffic, customized summary reports, and integrated security and network intelligence for drill down analysis, administrators easily identify internal and external attacks, network exposures and policy violations. The SMC also enhances network management through trend analysis, firewall and capacity planning, interdepartmental billing and performance monitoring.



### StealthWatch Management Console Benefits

- Centralized management, configuration and reporting for up to 25 StealthWatch flow collector appliances
- Real-time data correlation, traffic visualization and consolidated reporting
- Easily understood graphics with rapid drill-down to essential network behavior details

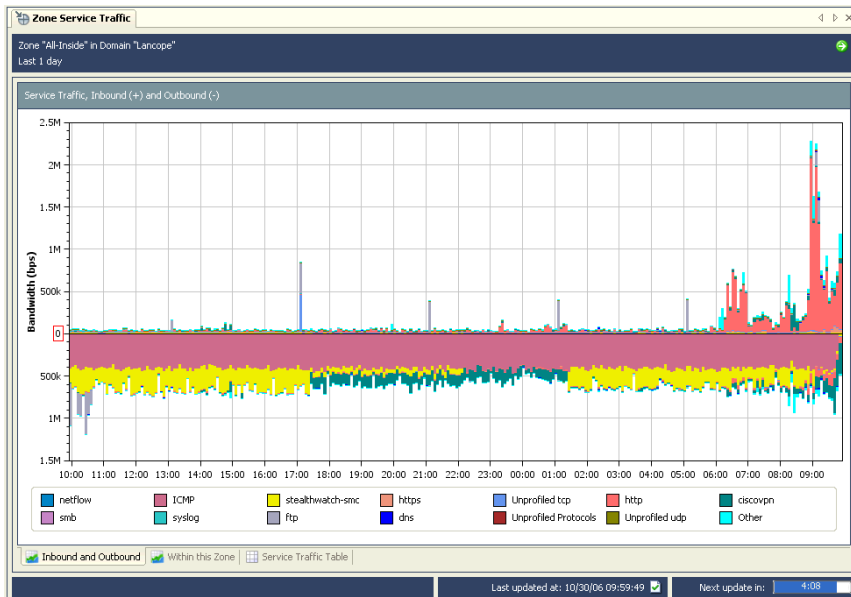
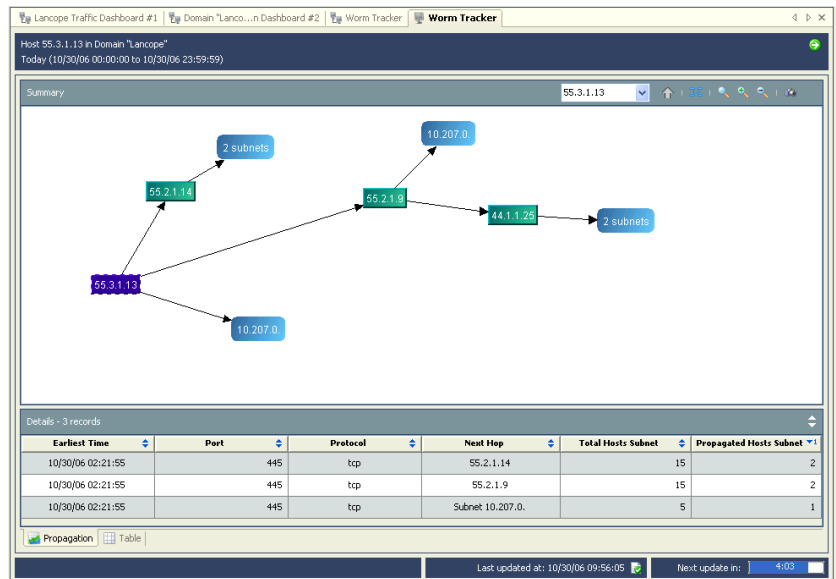


### Rich User Interface

With flexible views and powerful drill down analysis, the SMC provides rapid insight into the security and usage of the network. As a single point of reference for security and network intelligence, the SMC provides customized views, delegated operation and reporting of security, traffic accounting, interface utilization and user identity tracking.

### Worm Outbreak Visualization

Enabling rapid investigation and remediation of worm outbreaks, the SMC offers sophisticated flow visualization to provide immediate understanding of worm activity, propagation and impact. Additionally, point(s) of entry are identified to expedite incident resolution and fortify defenses against re-infection.



### Network Traffic Analysis

Graphically displayed network traffic relationships help network and security teams understand traffic patterns and identify deviations from normal network behavior. Real-time visualization aids the detection of DoS attacks, worms, reconnaissance and network misuse, as well as helps administrators identify network bottlenecks, spot malfunctioning network devices and perform capacity planning to optimize network performance.

## StealthWatch Management Console Features

- **Insightful real-time reporting**
  - Customizable XML-based reports include source/destination IP address, services, time period, traffic protocol and bandwidth
  - Useful for creating and assessing security policies; ensuring proper configuration of firewalls, servers and other network devices; identifying trends; anticipating and remediating problems
  - Flexible, SOAP-compliant API provides ready access to StealthWatch data from within Enterprise applications such as SIEM's, trouble ticketing systems and third party reporting systems
  - Fully-customizable dashboards and reports supported by 100+ unique reporting components
- **Point of View™ technology**
  - Provides a unique, customized view of the network for each IT role
  - Presents network engineers with router interface statistics, top talkers and trending reports
  - Presents security analysts with graphical reports of policy violations, worm outbreaks and other malware
- **Efficient centralized administration across distributed enterprise deployments**
  - Simplifies global deployment and remote administration for multiple StealthWatch flow collector appliances regardless of physical location
  - Provides streamlined integration between the StealthWatch System and standard network management applications
- **Customizable, flexible views of security and network events and behavior**
  - Rich graphical display of network traffic relationships and security activity, grouped by country of origin if so desired, helping administrators gain even more context to quickly identify traffic patterns and deviations from normal behavior
  - Aids detection of DoS and DDoS attacks, worms, pre-attack reconnaissance and network misuse — as well as network bottlenecks and malfunctioning devices
  - Provides critical visibility needed to ensure actual traffic passing through individual interfaces matches configured or desired traffic levels for each service
- **Drill-down analysis of security and network events**
  - Explores alarms, trends past and present host-level activity and detects suspicious network behavior enabling administrators to quickly prioritize and respond to attacks and mitigate damage
  - Correlates data across the enterprise for in-depth root-cause analysis and rapid recognition of network and security trends
- **Correlation of external events from syslog sources**
  - Employs a high-speed customizable syslog parser to facilitate integration with firewalls, IDS/IPS appliances and any other technology capable of exporting syslog messages
  - Events received are decoded, correlated with StealthWatch events and stored for later analysis in the SMC database
- **Redundant configuration**
  - Allows auxiliary deployment in a disaster recovery center or any other location
  - Provides uninterrupted access to critical network information in a time of crisis or system failure
  - Readily available in read-only mode to be activated by administrators for full access

## StealthWatch Management Console Appliance Options

**Standard** – 1U rack-mountable appliance available with up to 5 or 15 connections (may be upgraded to support unlimited connections).

**Enterprise** – 2U rack-mountable appliance with unlimited connections and three times the storage of the standard StealthWatch Management Console.

## Product Specifications

	SMC Standard - 1U	SMC Enterprise - 2U
Network	2 - 10/100/1000 MB, Copper Ethernet interfaces (only 1 used)	
Drive Capacity	300 GB	1000 GB - RAID5 <b>redundant</b>
Power	<b>Redundant</b> 670 Watt hot-plug power supplies  Auto-switching universal 110/220 Volts	AC configuration with standard <b>redundant</b> 750W hot-plug auto-switching universal 110/220V AC power supplies  DC configuration with redundant hot plug -48 to -60 V20 A DC power supplies
Chassis	1U Rack-mountable chassis  30.4" (77.2cm) D x 16.7" (42.6cm) W x 1.67" (4.26cm) H with bezel attached  Rack Weight 35.8 lbs (16.3 Kg), maximum configuration	<b>2U</b> Rack-mountable chassis  29.31" (74.4cm) D x 17.5" (44.43cm) W x 3.4" (8.64cm) H with bezel attached  Rack Weight 50.71 lbs (23 Kg), maximum configuration
Environmental	Operating Temperature: 10° C to 35° C (50° F to 95° F) Storage Temperature: -40° C to 65° C (-40° F to 149° F) Operating Relative Humidity (non-condensing twmax=29C): 20% to 80% non-condensing Maximum humidity gradient: 10% per hour, operational and non-operational conditions Storage Relative Humidity: 5% to 95% non-condensing (twmax=38C) Operating Vibration: 0.26G at 5Hz to 350Hz for 2 minutes Storage Vibration: 1.54Grms Random Vibration at 10Hz to 250Hz for 15 minutes Operating Shock: 1 shock pulse of 41G for up to 2ms Storage Shock: 6 shock pulses of 71G for up to 2ms Operating Altitude: -16 to 3,048m (-50 ft to 10,000 ft) Storage Altitude: -16m to 10,600m (-50 ft to 35,000 ft)	
Regulatory	FCC (U.S. only) Class A DOC (Canada) Class A CE Mark (EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3, EN60950) VCCI Class A UL 1950 CSA 950 EN 60950	

### About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

### Lancope Headquarters

3650 Brookside Parkway  
Suite 400  
Alpharetta, GA 30022

+1.770.225.6500 (US)  
888.419.1462 (Toll Free)  
+44 (0) 560 344 8075 (Intl.)

Website: [www.lancope.com](http://www.lancope.com)

E-mail: [sales@lancope.com](mailto:sales@lancope.com)

©2009 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. StealthWatch is covered by U.S. Patent Nos. 7,290,283; 7,185,368; 7,475,426; 7,512,980 and other U.S. and foreign patents pending.

DS07292010