Lancope

Behavior-Based IDS: StealthWatch™ Overview and Deployment Methodology

Lancope
3155 Royal Drive, Building 100
Alpharetta, Georgia 30022

Phone: 770.225.6500
Fax: 770.225.6501

www.lancope.com
techinfo@lancope.com

StealthWatch™ Overview

Lancope's flagship product is StealthWatch, a behavior-based intrusion detection and threat management system. StealthWatch utilizes a multi-dimensional approach that includes:

- Flow-based statistical analysis
  - high speed event correlation
  - denial of service detection
  - reconnaissance detection
  - network based worm and trojan detection
  - malfunctioning network applications
- Traffic management
  - internal and external network misuse
  - peer-to-peer applications
  - capacity planning
  - network troubleshooting and management
- Policy management
  - unauthorized access
  - rouge applications (unauthorized web-servers, gaming servers, etc.)
  - firewall policy auditing and management
  - change management
- Forensics auditing and accounting
  - full audit trail of network activity
  - detailed host activity reports

The functionality listed above is accomplished without the need for signatures or a complex database of attack fingerprints.
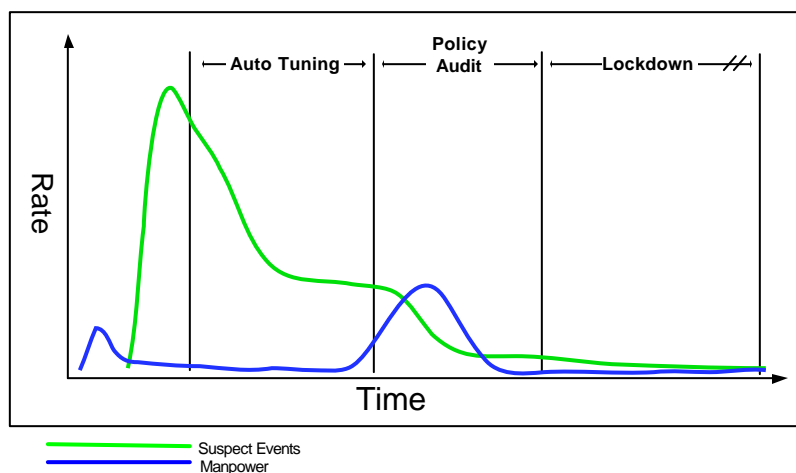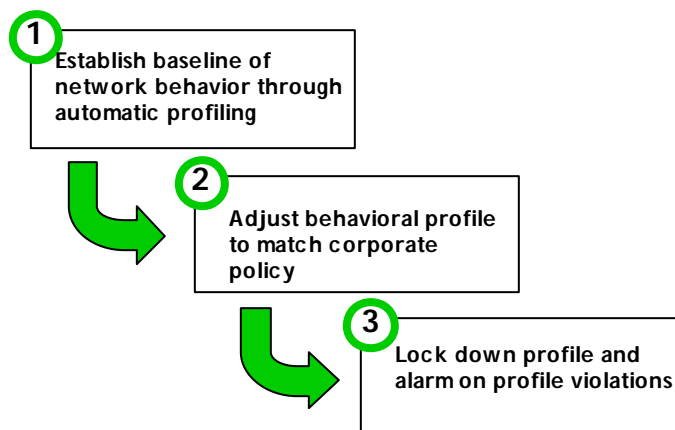
Appliance Configuration

StealthWatch is a self contained, 1U network appliance. Each appliance offers two passive network interfaces that can be connected to a hub, mirror port, or in-line Ethernet tap.

Two StealthWatch appliance configurations are available:
1. StealthWatch M-100
   - 1U rack mounted 100Mb capable appliance
   - two 10/100 copper interfaces (capture ports) & one 10/100 interface (management port)
2. StealthWatch G-1
   - 1U rack mounted gigabit capable appliance
   - two gigabit fiber interfaces (capture ports) & one 10/100 interface (management port)

Deployment Methodology and Theory

StealthWatch operates by establishing a behavioral profile of network activity and usage. During initial installation, an auto-tuning period will take place, allowing StealthWatch to "auto-tune" host specific thresholds and settings. Upon completion of this period, previously compromised hosts and policy violators will be remedied. Once the profile is complete and final manual tuning has taken place, the behavioral profile is "locked down." A customizable alarming system can be configured to send email, SNMP alerts, and pager notifications when violations occur.

1 Establish baseline of network behavior through automatic profiling

2 Adjust behavioral profile to match corporate policy

3 Lock down profile and alarm on profile violations

The use of auto-tuning technology greatly reduces the need for an expensive, time-consuming, Intrusion Detection System (IDS) deployment strategy. The diagram above shows the typical manpower requirements of a StealthWatch installation. Notice the sharp decline of suspect events and manpower requirements once the auto-tuning period has ended.
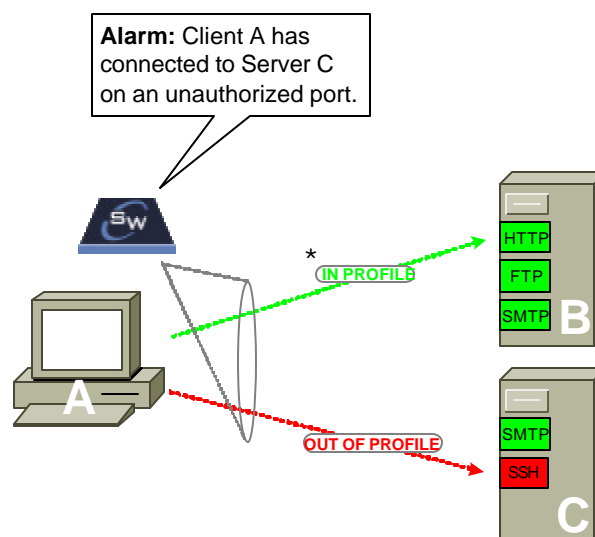
Behavioral Profiling

Host Profiles

Host profiling is the process of passively identifying and categorizing network resources. Acting as a sort of "passive port scanner," StealthWatch monitors network hosts' activity and builds a profile for each network host. This profile includes the client and server connections created by each network host.

Host profiles can be dynamically built, auto-tuned, or manually configured using the Host Profiler.

Once configured, host profiles can be locked in place. If necessary, StealthWatch will alarm on infractions to the established profiles. This becomes especially effective in DMZ or other controlled server environments. Host profiling provides an outstanding mechanism for detecting network trojans, worms, and other unauthorized activity. StealthWatch provides a number of canned reports that can be used to enforce acceptable use policies as well as detect rogue or unauthorized network activities.

Host profiles are tied directly to the StealthWatch flow analysis engine. Host profile entries such as a UDP port 53 server (DNS) will cause StealthWatch to modify its algorithms and assumptions when analyzing network flows. Another example includes that of TCP port 25 (SMTP). If StealthWatch sees SMTP traffic in a flow, special analysis for SMTP will be used to validate mail server behavior.

Alarm: Client A has connected to Server C on an unauthorized port.

HTTP
FTP
SMTP
B

* IN PROFILE

SMTP
SSH
C

OUT OF PROFILE

A

Traffic Profiling

Packet rate, bandwidth consumption, protocol usage, and traffic history statistics provide an extremely powerful tool for the security administrators as well as the network teams. In many ways, StealthWatch doubles as not only a security tool, but also a powerful network management platform.

StealthWatch allows for host-by-host traffic thresholds as well as system wide bandwidth policies. Traffic profiling is useful in detecting Denial-of-Service (DOS) conditions, bandwidth "hogs," and many other resource related threats.

Similar to host profiles, traffic profile thresholds are factored in to the flow based statistical analysis algorithms. Traffic profiles can be manually configured or automatically configured during the auto-tuning process.

Alarm: Server A is running at 1050Kbps, Server A's traffic threshold is 1000Kbps.

500Kbps

50Kbps

500Kbps

A
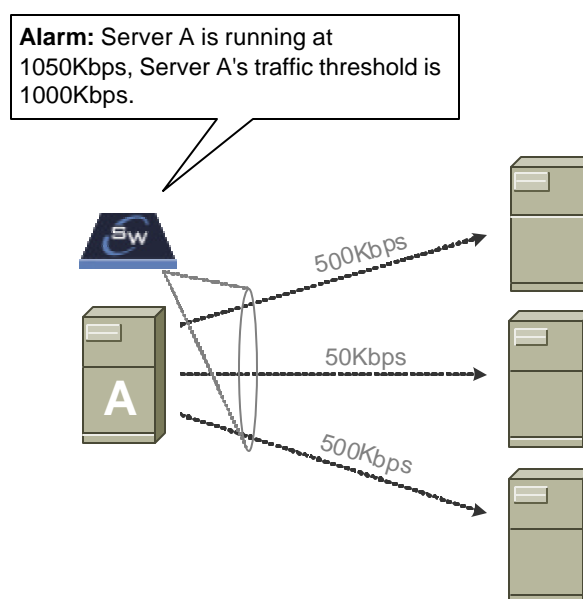
High Resolution Manual Tuning

By default, StealthWatch performs dozens of calculations on flow data that result from host activity. Knowing that there are always aspects of network behavior that cannot be accounted for by intelligent alarming or auto-tuning, StealthWatch allows for high-resolution exceptions from the flow analysis calculations. This means that any behavior, regardless of the type, can be exempted if the behavior is authorized.

Flow-based Statistical Analysis

StealthWatch utilizes a unique, patent pending flow-based packet capturing and analysis engine. As Ethernet frames are received through one of the two promiscuous interfaces on the StealthWatch appliance, these packets are fed into a flow analysis engine that separates and categories the active data flows.

Once these flows have been properly categorized, StealthWatch performs periodic analysis of the collected data, checking host profiles, traffic profiles, and system-wide threshold settings to verify the flows satisfy the parameters of the established behavioral profile.

Nefarious traffic is then identified and reported. As patterns emerge and suspect flows are identified, StealthWatch begins to accumulate *Concern Index* points for the suspect host.
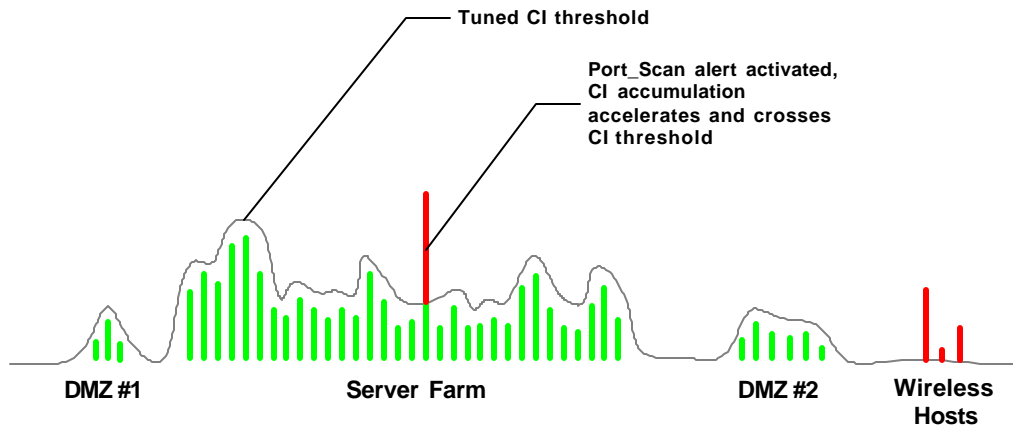
As a host's Concern Index increases, StealthWatch begins to raise alarms to notify an administrator of the host's activity.

Each network host has an independent Concern Index threshold. During the auto-tuning process, or manually through the StealthWatch host profiler, a host's Concern Index threshold will be set to its optimal amount.
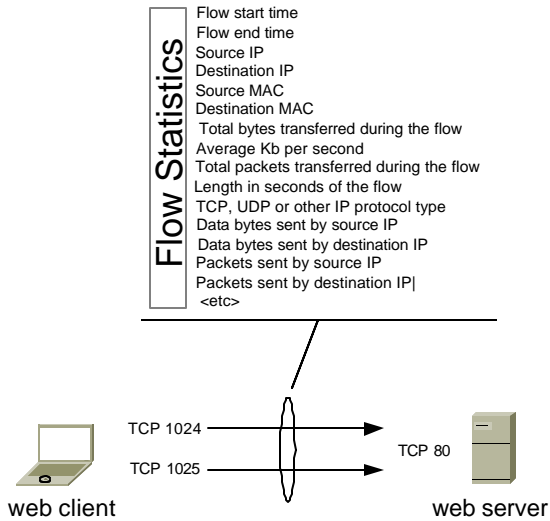
The Concern Index provides a detailed mechanism of prioritizing and reporting network threats. When used in conjunction with signature-based IDS, the Concern Index greatly decreases the administrative load and rate of false positives normally seen in signature-burdened IDSs.
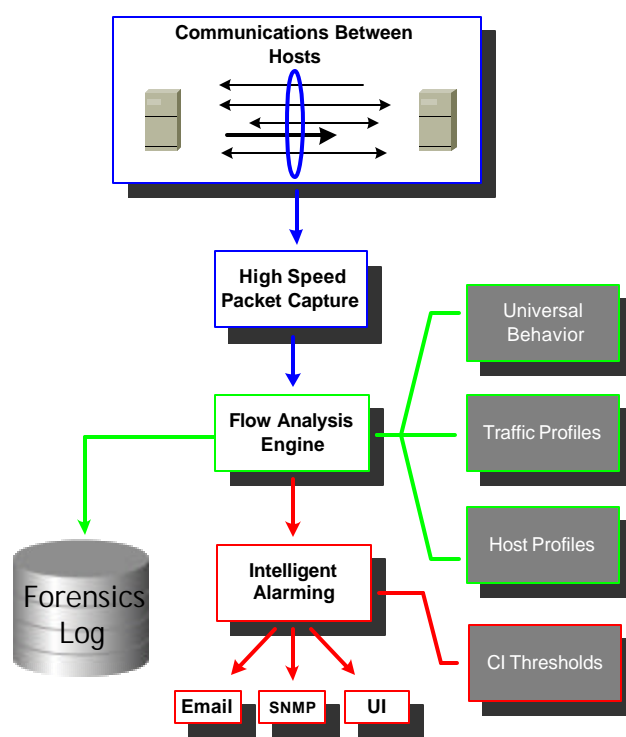
The diagram below shows a logical representation of tuned concern index thresholds across several server farms and an unknown wireless network.

Tuned CI threshold

Port_Scan alert activated, CI accumulation accelerates and crosses CI threshold

DMZ #1   Server Farm   DMZ #2   Wireless Hosts

Once StealthWatch has processed a flow and the communication between two hosts have ceased, the flow data is archived to a log for up to 30 days. This flow data provides a detailed audit trail of network activity that can be used to research suspect network activity or build evidence against an internal or external network user.

Flow Statistics

Flow start time
Flow end time
Source IP
Destination IP
Source MAC
Destination MAC
 Total bytes transferred during the flow
Average Kb per second
Total packets transferred during the flow
Length in seconds of the flow
TCP, UDP or other IP protocol type
Data bytes sent by source IP
 Data bytes sent by destination IP
Packets sent by source IP
Packets sent by destination IP|
 <etc>

The diagram at left shows a portion of the data points accumulated for each flow. A "flow" is defined as a connection between two hosts that consists of one server port and any number of client source ports. The diagram shows a typical flow involving a web client and a web server.

TCP 1024
TCP 1025
TCP 80

web client   web server

- 6 -

StealthWatch Management

Key to the success of StealthWatch has been the StealthWatch Management Console (SMC). StealthWatch provides a wealth of data that can be managed in two ways:

1. Integrated web dashboard

    Each StealthWatch appliance comes with its own integrated web server and a lightweight web dashboard. The SSL based web dashboard can be used to administer a single sensor or can be used should the sensor or the admin lose contact with the SMC. The web dashboard is fully featured and provides nearly all the management capability of the SMC.

2. Appliance-based StealthWatch Management Console

    The SMC provides enterprise level management of one to more than 20 StealthWatch sensor appliances. The SMC allows for management of complex networks and profile data through the use of a network group hierarchy. The SMC replaces (but does not remove) the web dashboard and allows for single interface management of the agency's StealthWatch sensors.

    The SMC is deployed as a separate 1U appliance. Setup and configuration are similar to that of a StealthWatch sensor. All database resources, software, and the desktop client application are embedded within the SMC appliance. The desktop client application is dynamically "pulled" to the administrator's machine when the SMC application is launched (by clicking on a web link).

    The diagram at rights portrays a high-level overview of the SMC's three-tier hierarchy.

    It is important to note that the SMC to StealthWatch bandwidth is extremely predictable and very efficient. Inter-StealthWatch communications are kept to a minimum.

- 7 -
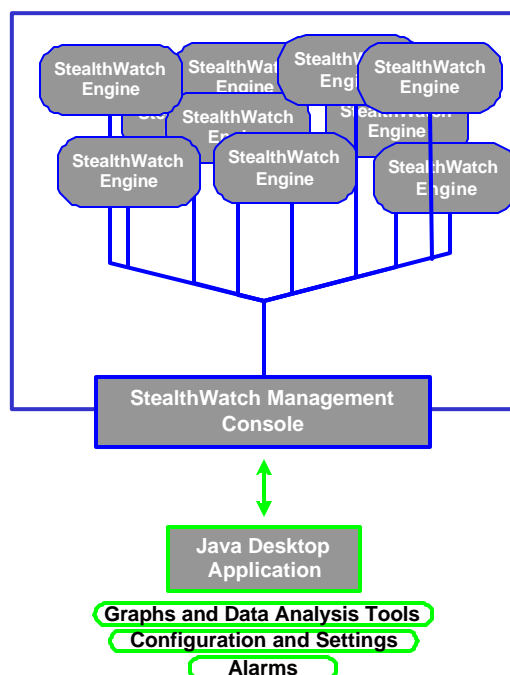
About the Author

As a Security Engineer with Lancope, Adam Powers has over eight years of operational and engineering experience in enterprise IP security technologies and specializes in UNIX and IP networks. His expertise includes data center network design, content delivery networks, and enterprise network security planning and management.

About Lancope

Lancope is the provider of Advanced Threat Management solutions designed to combat today's advanced hacking exploits and corporate network misuse on enterprise networks. The company's flagship product, StealthWatch, is an advanced Intrusion Detection System that enables intelligent alarming, provides advanced network surveillance, operates at Gigabit speeds, recognizes unknown threats, and creates a forensic trail of network activity. StealthWatch recently received the Innovation In Infrastructure Award (i3) in the security category from the editors of eWeek Magazine and PC Magazine at Spring NetWorld+Interop 2002 and was named "Most Impressive" by eWeek in 2001. Installed on the networks of Fortune 1000 organizations and government entities, StealthWatch protects the critical assets of today's largest enterprises.

For more information, contact techinfo@lancope.com or visit http://www.lancope.com.