



## ipANGEL™ Anti-Vulnerability Solution

Lucid Security's ipANGEL marks a departure from the conventional wisdom regarding security solutions in the intrusion arena. The philosophy during the design phase focused on proactively choosing ipANGEL's limitations:

- Operates exclusively with FireWall-1®
- Does not duplicate FireWall-1's functionality
- Ignores traffic that will not harm the systems being protected

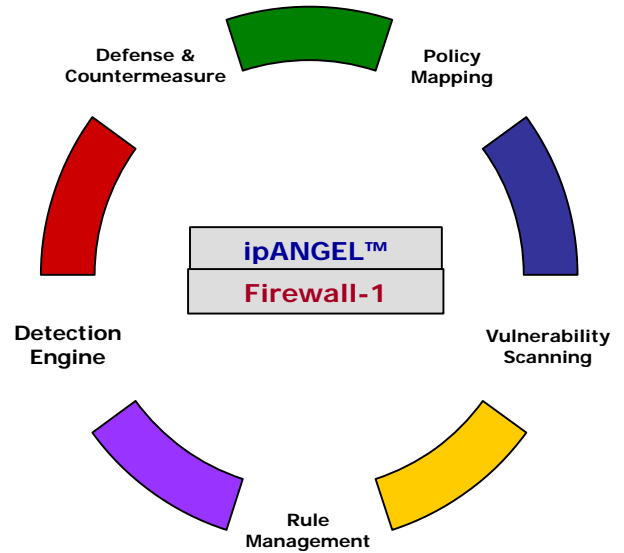
The designers of ipANGEL created a sophisticated intrusion product that is neither a vulnerability assessment tool, nor an intrusion detection system, yet it incorporates both technologies.

ipANGEL is low-maintenance; providing real-time defense that is affordable and easy to use. Coupled with the capabilities of FireWall-1, ipANGEL provides **complete** protection against all network and application attacks.

For more information and a complimentary white paper on Lucid Security's ipANGEL please visit <http://www.lucidsecurity.com>.

### Automated Features

- Vulnerability scanning
- Intrusion detection
- Self-tuning
- Auto-update of attacks and rules
- Real-time attack protection



### Anti-Vulnerability – a new approach

ipANGEL provides protection from attacks that exploit vulnerabilities found on a network. It is designed to defend against **relevant** attacks. These are the attacks that will compromise network operations.

ipANGEL automatically queries FireWall-1 to gather network topology information and tests accordingly to determine the network's vulnerabilities. Then, ipANGEL and FireWall-1 – via Check Point's Suspicious Activity Monitor (SAM) API – actively defend against exploits to those vulnerabilities in real time.

### ipANGEL Benefits:

- Affordable
- Easy to deploy and maintain
- Always up-to-date
- Ongoing vulnerability protection
- Enhanced perimeter security



ANGEL™  
0110010100100100111010100101101



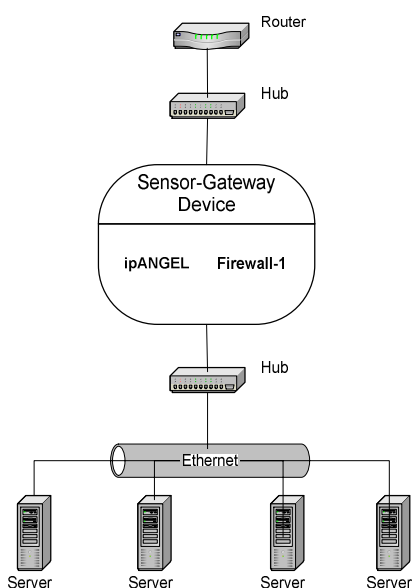
## Deployment Options

*ip*ANGEL can be deployed in either a “standalone” or a “sensor-gateway” configuration. Both are **OPSEC certified** and tightly integrated with Check Point FireWall-1.

## Sensor-Gateway

Lucid Security's *ip*ANGEL is the first and only IDS/IPS software to be OPSEC certified as a **sensor-gateway** solution with Check Point FireWall-1. As a sensor-gateway, *ip*ANGEL operates as an add-on module and is installed on the same hardware device as FireWall-1.

## Sensor-Gateway (Inline) mode



## Five (5) engines that power *ip*ANGEL:

- Firewall-1 Policy mapping engine (CPMI)
- Vulnerability Scanning engine
- Rule Correlation & Management engine
- Intrusion Detection engine
- Defense & Countermeasure engine (SAM)

## CPMI – Check Point Management Interface

*ip*ANGEL queries the firewall for policy information via Check Point's CPMI API. *ip*ANGEL determines which IP addresses (and ports) will be automatically scanned and instructs the detection engine to listen for attacks on specific IP addresses (and ports) based upon information in the firewall policy.

## SAM – Suspicious Activity Monitor

*ip*ANGEL instructs the firewall to “drop & inhibit” attacks via Check Point's SAM API. When *ip*ANGEL sees a relevant attack against a vulnerable host, it instructs FireWall-1 to drop & inhibit the connection. The “inhibit” time to live (TTL) can be set via *ip*ANGEL's user interface.

## System Requirements (Minimum)

Memory	256 MB RAM
Network	Two Ethernet/Fast Ethernet
Internal CD	CD-ROM
Hard Drive	125MB Free Disk Space



Lucid Security Corporation  
124 S. Maple Street, Suite 200  
Ambler, PA 19002 USA  
T +1.215.371.3300  
F +1.215.371.1753