



Lucid Security's *ipANGEL*™: Extend the capabilities of FireWall-1® and SmartDefense™

ipANGEL, coupled with the capabilities of FireWall-1 and SmartDefense provides **complete** protection against all network and application attacks.

SmartDefense builds upon the powerful capabilities of Check Point's Stateful Inspection security engine to provide advanced security against both known and unknown attacks, including:

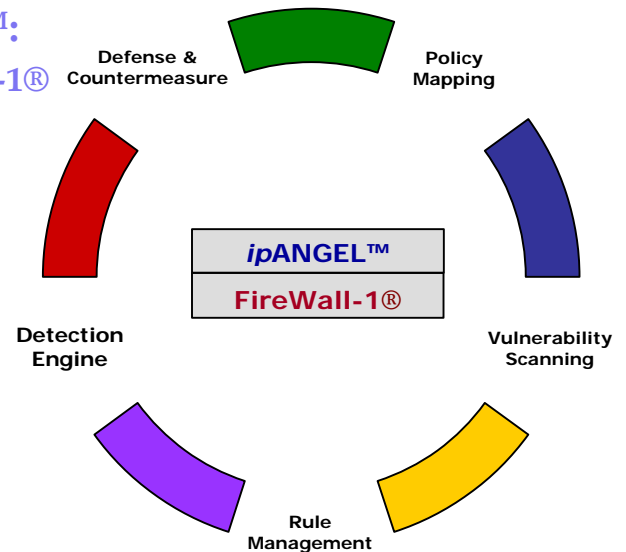
- IP Attacks - including, IP spoofing and IP fragmentation
- Denial of Service (DoS) Attacks - including SYN flood and LAND
- Web & Application Vulnerabilities - including trojan horses, DNS attacks and worms such as Nimda and Code Red
- Network Probing - including port scanning and service scanning

Vulnerability Shield – 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.

Automated Features

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



The Power of Integration

ipANGEL integrates with FireWall-1 via several of Check Point's OPSEC APIs in order to leverage the firewall's strengths and avoid duplicating the functions performed by FireWall-1.

ipANGEL automatically queries FireWall-1 to gather network topology information and tests accordingly to determine the network's vulnerabilities. Then, *ipANGEL* and FireWall 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



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

Content Filtering (URI Filter)
Allowed FTP Commands
FTP Bounce
Allowed SMTP Commands
Allowed SMTP Parameters
HTTP Format (ASCII headers only)
HTTP Format Sizes
HTTP worm catcher
Protocol Anomalies
DNS Verification (UDP)
Malformed Packets
IP fragmentation
Small PMTU
SYN Attacks
Successive Multiple Connections
Sanity Checks
FTP Content
Packet Sanity
Sequence Verification



Technology	SmartDefense	ipAngel	Combined
Automated Rule Management			
Automatic Rule Activation		●	●
Automatic Rule Deactivation		●	●
Automatic Updates			
Attack Detection Signatures	●	●	●
Vulnerability Testing Signatures		●	●
Correlation Database		●	●
Attack Protection			
Application-specific Vulnerabilities	●		●
Back Door and Remote Administration	●		●
Content Filtering	●		●
Denial of Service	●		●
DNS Attacks	●		●
Hidden File Extensions	●		●
IP Spoofing	●		●
Mobile Code (Java, JavaScript, Active-X)	●		●
Protocol Anomalies	●		●
Port & Service scanning	●		●
Trojan Horses	●		●
Vulnerability Shielding			
Backdoor vulnerabilities		●	●
Finger abuses & vulnerabilities		●	●
FTP vulnerabilities		●	●
Gain root or shell remotely		●	●
HTTP vulnerabilities		●	●
Novell vulnerabilities		●	●
NIS vulnerabilities		●	●
Other Misc. vulnerabilities		●	●
Remote file access vulnerabilities		●	●
RPC vulnerabilities		●	●
Improper Settings		●	●
SMTP vulnerabilities		●	●
SNMP vulnerabilities		●	●
Windows vulnerabilities		●	●
Vulnerability Detection			
Backdoor vulnerabilities		●	●
Denial of Service		●	●
Finger abuses & vulnerabilities		●	●
FTP vulnerabilities		●	●
Gain root or shell remotely		●	●
HTTP vulnerabilities		●	●
Novell vulnerabilities		●	●
NIS vulnerabilities		●	●
Other Misc. vulnerabilities		●	●
Remote file access vulnerabilities		●	●
RPC vulnerabilities		●	●
Improper Settings		●	●
SMTP vulnerabilities		●	●
SNMP vulnerabilities		●	●
Windows vulnerabilities		●	●

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



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