



Lucida SecurEdge™

Intrusion Detection & Traffic Analysis



The Security Problem

Network security attacks are increasing in frequency, intensity, and sophistication. And no enterprise is immune from these malicious attacks. One problem most companies face when planning for more complete security coverage is the high cost and complexity of today's intrusion detection (IDS) systems. This results in a dilemma between IT budgets and resources on the one hand, and the need for stronger enterprise network security on the other. Another key issue is the lack of visibility; that is, the lack of a complete picture of the network traffic and flow dynamics resulting from a security event.

The SecurEdge™ Solution

Lucida SecurEdge™ is a powerful, low-cost IDS system. SecurEdge™ is low-cost because it leverages open source and industry standard software. SecurEdge™ is powerful because it combines best-of-breed, award-winning open source IDS and IP traffic and flow analysis software tools—Snort, ntop, nProbe—with Lucida's powerful, cross-platform server and easy-to-use interface. SecurEdge™ includes a management console, which uses an intuitive Web-based, Excel spreadsheet interface for reporting, alarms, and remote sensor management.

Do you have the full visibility into your network you need to spot unusual or unhealthy IP activity before it becomes a critical security event? Is the high cost and complexity of IDS systems keeping you from achieving the level of security coverage you really need to meet today's security threats? How much more protected does your network need to be? Are you willing to wait for the next serious hacker intrusion to find out?

The Power of Visibility

SecurEdge™ goes beyond basic intrusion monitoring by showing related traffic and netflow data in the same view for a more complete picture of threats and events. SecurEdge™ also allows you to set e-mail/pager alerts so that you are instantly notified when a security policy has been violated or has reached a critical threshold.

SecurEdge™ System Features

SecurEdge™ is a powerful, high-value network intrusion detection and network traffic analysis software suite for standard IP networks. The SecurEdge™ system includes server software, sensor agents and sensor software on sensor appliances, located near key access points.

Server:

- Small footprint server, includes an applications server, Web server, sensor manager, Lucida Insight® server and database.

Management Console:

- Web-based, Excel interface
- Remote management of sensors
- Policy management
- Manage sensors by groups
- Report & template design
- Alarm priority and notification settings
- Server management

Sensors:

- Sensor appliance
- SecurEdge™ sensor agent software
- Sensor probes: Snort, ntop, nProbe

Security Alarms:

- Priority 1-5 rule-based alarms. Define security threshold alarms and who will be notified by e-mail, cell phone or pager message.

Intrusion Detection:

- Signature, protocol, and anomaly-based inspection methods

Report Wizards:

- You decide what data you want to view when, through easy-to-use wizards, without requiring SQL scripts or programming.
- Define report templates or create ad-hoc reports for instant analysis.

Excel Power:

- Freely manipulate report values in an Excel spreadsheet, adding any standard Excel formulas for empowered analysis, data correlation and decision-making
- Store your work locally as an Excel spreadsheet or on the SecurEdge™ server for archiving, sharing, or future reference.



Administration:

- Full user administration and access privileges settings

SecurEdge™ Benefits

Added Protection:

- Greater sensor distribution, density and coverage possible at a lower cost
- Correlate netflow, protocol, and service data in a single Web-based view for a more complete security picture.

Optimized Security:

- Fine-tune your security policies for the level of protection you need
- Fast analysis through easily customized reports

- Define your own exception-based alerts for instant notification of business opportunities and threats

Decreased Costs:

- Leverage and not replace your existing security investment by using SecurEdge™ as a low-cost supplement for your current infrastructure or to extract critical data from other security systems, correlate it, and deliver it to you in a customizable Web-based security management dashboard.
- Improve productivity by automating manual tasks, which lets you accomplish more in less time

Spend less time writing scripts and more time analyzing security events

Platform Requirements

Server Hardware :

- Pentium IV 1.4 GHz, 512K cache, 512 MB Memory, 3 GB Hard Disk.

Server Software :

- Windows NT 4.0/2000/XP
- -or- Red Hat Linux (9.0)
- Lucida Insight® server
- DBMS (PostgreSQL, Oracle8i/9i)

Client Hardware :

- PC Pentium II 400 MHz

Client Software :

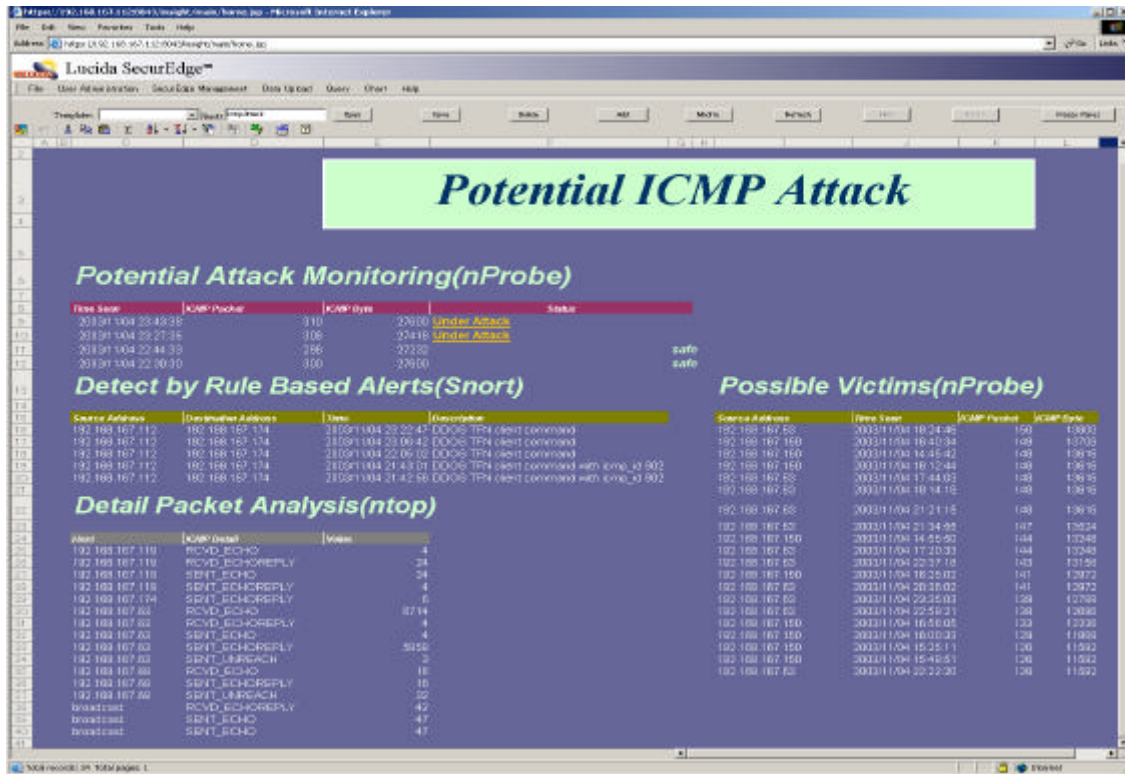
- Windows NT 4.0/2000/XP
- Internet Explorer 5.5+
- Office 2000 Web component

Sensor Hardware :

- PC Pentium II 400 MHz 256M Memory, 2GB Hard Disk

Sensor Software :

- Red Hat Linux (9.0)
- SecurEdge™ Agent
- Snort, ntop, nProbe



SecurEdge™ The Power of Visibility