

Lucida SecurEdge™ Network Security Management

Technical Overview





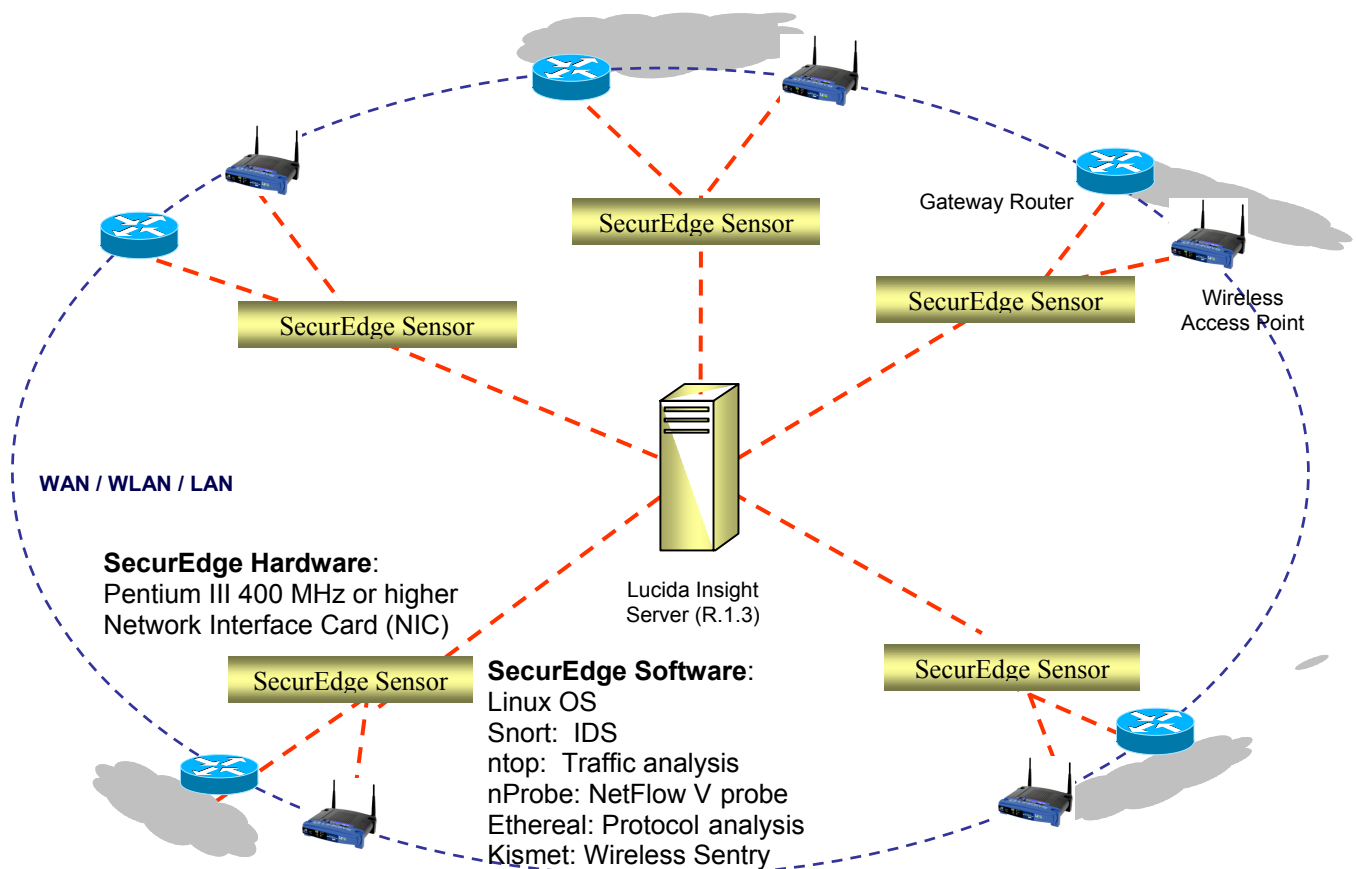
SecurEdge™ Technical Overview

Lucida SecurEdge™

SecurEdge™ is a powerful, high-value network intrusion detection and network traffic monitoring software suite for both standard IP and 802.11 wireless networks. SecurEdge™ comprises server, client, and sensor software, and the suite is designed to run on inexpensive PC appliances strategically located near key access points and gateway routers, with a centrally located server.

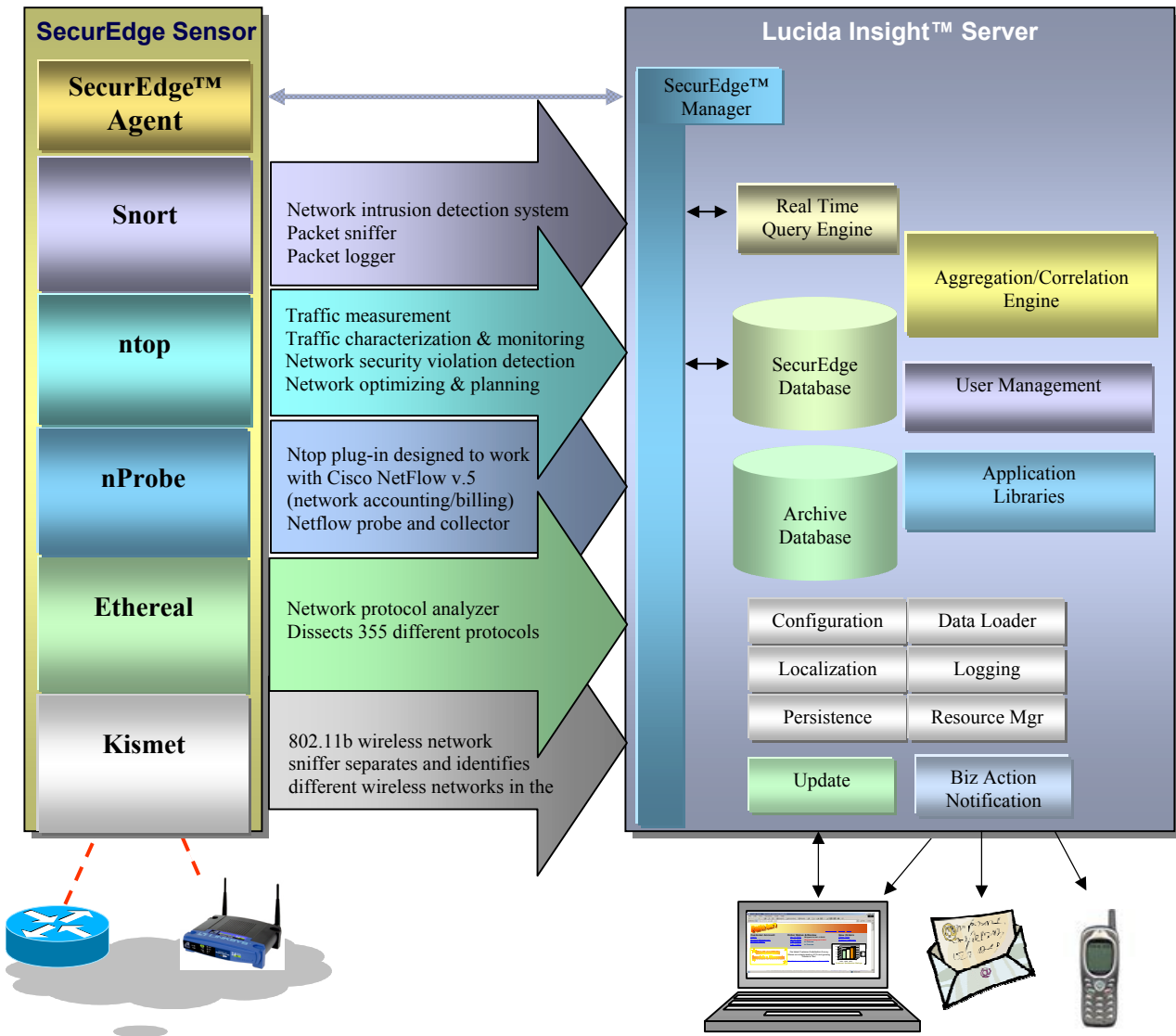
SecurEdge™ combines the best of breed open source tools available today—Snort, nProbe, ntop, Kismet and Ethereal—with Lucida Insight™, a leading network and business performance management platform.

SecurEdge Network Architecture





SecurEdge™ Product Architecture



SecurEdge & Lucida Insight™

Lucida SecurEdge is built on Lucida's flagship product, Lucida Insight™, which is a versatile software platform for extracting business-critical data from across corporate, external, and network data-source boundaries and securely delivering real-time, Web-based spreadsheet, graphical, and text views.

Lucida Insight™ is a multi-tiered, client-server architecture, comprising a full set of business performance management and information delivery functions. The product is designed around open and industry standard components and protocols—XML, J2EE, SQL, HTTP/HTML, SOAP, JBoss, PostgreSQL, Apache, JDBC—for lower cost and ease of installation, integration, customization, and maintenance.



SecurEdge™ System Description

The SecurEdge™ system provides a scaleable, reliable, high performance client-server architecture to deliver data from remote network sensors and other data sources in real-time. The core SecurEdge™ system consists of the following major components:

SecurEdge™ Sensor

The SecurEdge™ Sensor comprises a SecurEdge Agent to manage the sensor-server transactions, Linux OS, and a bundle of open source software applications running on a standard PC appliance. The software includes Snort, ntop, nProbe, Ethereal, and Kismet. The following measurements and data are generated by the SecurEdge Sensor and stored in the SecurEdge database:

- **Snort:** Intrusion events and priority 1-5 alarms as specified in the Snort rules description language
- **ntop:**
 - Traffic Measurement: data sent/received by host; packet classification; IP multicast; TCP session history; UDP traffic; TCP/UDP services used; OS type; bandwidth usage %; traffic distribution; IP traffic distribution; local network usage; global traffic statistics.
 - Traffic Characterization & Monitoring: use of duplicate IP addresses; subnet router identification; local hosts with NICs set in promiscuous mode; service misuse detection; protocol misuse; excessive bandwidth utilization.
 - Network Security Violation Detection: portscan, spoofing, spy, trojan horse, and denial of service detection.
 - Network Optimization & Planning: identify unnecessary protocols and sub optimal routing
- **nProbe:**
 - NetFlow v.5 header format data: version; count (flows in this packet); device uptime since boot; total sequence count of flows seen; flow-switching engine type; slot number.
 - NetFlow v.5 record format data: IP address for source, destination and next hop router; SNMP index of input and output interfaces; packets in flow; Layer 3 bytes in flow packets; SysUptime for first and last packets received; TCP/UDP source and destination ports; cumulative OR and TCP flags; IP protocol and ToS types; source and destination autonomous system numbers; source and destination prefix mask bits.
- **Ethereal:** Protocol Analysis: Ethereal resides on the SecurEdge™ sensor, but does not integrate directly with the Lucida Insight database at this time.
- **Kismet:** Wireless sentry: Kismet resides on the SecurEdge™ sensor, but does not integrate directly with the Lucida Insight database at this time.



SecurEdge™ Client

The SecurEdge™ Client is thin and lightweight, leveraging the most popular desktop application, Microsoft Excel spreadsheet. The spreadsheet runs within a standard web browser and can pull data from various data sources in real-time according to user-defined data collection schedules. Users can use standard Excel formulas to manipulate this real-time data and save their spreadsheets on the server or on their workstation as an Excel file. Clients can also specify actions to be taken when a particular data change or event occurs. These actions can vary from sending e-mail to initiating complex workflow processes. Also the users can create their own charts using standard Excel charts components available through the SecurEdge Client.

SecurEdge™ Manager

SecurEdge™ Manager allows the user to control one or more SecurEdge Agents. Furthermore, SecurEdge Agents can be combined into user-defined groups so that they can be managed as a single unit. The SecurEdge Manager can:

1. Group SecurEdge Agents into groups
2. Control individual agents and/or agent groups
3. Collect data from individual agents and/or agent groups.
4. Correlate data received from SecurEdge Agents and store it in the Lucida Insight™ database.

Once the data is collected in the Lucida Insight database, users can use Insight's query features to view and analyze the data.

SecurEdge Manager can remotely and automatically upgrade sensor appliances, leveraging Read Hat Enterprise Network (RHEN) software to upgrade the sensor OS and apply patches.

RHEN will run in Hosted/On-site mix mode. Using this architecture, selected OS upgrades and patches are downloaded on to a Proxy server at the customer site. All the appliances then connect to this proxy server to get updates.

Lucida should approve all the sensor upgrades to ensure that all future sensor software versions are compatible with the SecurEdge™ software. Lucida will verify the compatibility of the new sensor software and provide an RPM that can be used with the RHEN system upgrade architecture.

Lucida Insight™ Server

The SecurEdge™ system is built on the Lucida Insight™ high performance, distributed, multi-threaded server, which can pull data from SecurEdge sensors and other data sources and directly update interested clients. Clients can subscribe to changes in these data points, and the server will update the SecurEdge™ Client whenever the data changes. Server security provides user authentication, role-based authorization and digital encryption of any data transfer.

The server also provides the ability to monitor user subscriptions, even if the user is not currently logged into the system, as well as the ability to process those subscriptions for various actions, including business activity alerts.



SecurEdge™ Technical Overview

- **Data Collector**

The data connectors provide connectivity to various data sources and to the Lucida Insight™ server. These data sources include real-time networks, database systems, and other enterprise information systems. Clients can use these data connectors to specify the source of their data. Once the clients subscribe to the data they want using these data connectors, the SecurEdge Live Update component will update the SecurEdge Client whenever the subscribed data changes. The data connectors are implemented using the Data Collector framework.
- **Aggregation/Correlation Engine**

Lucida Insight™ is able to aggregate and correlate key data, as it is stored in the Lucida Insight™ database. Additionally, the user can aggregate and correlate any data displayed on the client simply by applying standard Excel formulas.
- **Biz Action Notification**

Lucida Insight™ provides an easy-to-use wizard for defining alarm thresholds, conditions, actions to be taken (e.g., e-mail, pager, cell phone), and who will be notified when a defined threshold or condition is true.
- **Scheduler**

Lucida Insight™ provides a framework to measure various characteristics of the enterprise. The measurement framework can be used to schedule measurements on assets. The user can implement a particular calculation on a measurement and schedule it using this framework. The measurement framework also supports aggregations, distributed schedulers, etc.
- **Query & Report Wizard**

The Lucida Insight™ Query Wizard provides a simple and friendly means for generating sophisticated database queries and reports. This query generation tool works with the subscription mechanism to identify the database related data sources the user is interested in. The user provides only high-level logical information, in response to the Query Wizard prompts. The Query Engine then maps this subscription information onto physical tables, views and columns and generates dynamic queries.
- **Data Loader**

Data Loader is used to load data into the Lucida Insight™ database.
- **User Administration Module**

The User Administration Module defines the user profile and permissions; that is, actions an individual user is allowed, or not allowed, to do. For example:

 1. User Administration allows a user with administrative privileges, to add, modify, and delete users and user's profiles.
 2. Server Management manages SecurEdge Servers, including startup, shutdown, etc.
 3. Schedule Management defines various measurement schedules.
 4. Database Management is used for database management.



SecurEdge™ Technical Overview

- **Other System Components**

The SecurEdge™ system contains several other components which can be used to customize and extend it. Some of these components are:

1. **Localization:** SecurEdge™ provides “out-of-the-box” support for English, Japanese and Chinese. This support includes a localized user interface and database. Other languages can be easily added using the SecurEdge Localization Framework.
2. **Persistence:** SecurEdge™ provides a database independent persistence layer to interact with underlying databases. The User can change the database without making any changes to the SecurEdge Platform.
3. **Logging:** SecurEdge™ provides an extensive logging mechanism to audit and track system activities.
4. **Resource Management:** SecurEdge™ provides efficient management of system resources, such as database connections, threads, files, etc., to maximize performance and scalability.

System Requirements

	Hardware	Software
Server	Sun UltraSPARC 300 MHz (1-2 CPU)	Solaris8
		Windows NT 4.0
		Windows 2000
	PC Pentium III 400 MHz (1-2 CPU)	Windows XP
		Linux
Client		Win 2000/XP/CE + Internet Explorer 5.5 + Microsoft Office 2000 Web component

Lucida Background

Lucida develops simple yet powerful software solutions for the real-time aggregation and Web delivery of business-critical information to fully optimize business performance and empower your best business decisions.

Headquartered in San Jose, California, Lucida, Inc. is a privately held company. Founded in 2000, Lucida also has an office in Tokyo, Japan, with a presence in Europe and Asia.

Lucida Inc...2870 Zanker Road...San Jose, CA 95134...408-546-2100... www.lucida.com