



astaro
internet security

[Astaro Firewall](#)

Network Security Whitepaper

Using Integrated Security Platforms to Improve Network Security and Reduce Total Cost of Ownership

Implementing complete network security, including firewalls, VPN, content filtering, virus protection, and spam filtering for resource-constrained organizations.

Version: 1.00

Release date: October 24, 2003

Author: Al Cooley, BSEE: WPI, MBA: University of Michigan,
Advanced Studies in Computer Engineering: Boston University



Reducing Network Security Total Cost Of Ownership

Astaro www.astaro.com info@astaro.com
Pfinztalstrasse 90, 76227 Karlsruhe, Germany
67 S. Bedford Street #400W, Burlington MA, 01801 USA

Table of Contents

Reducing Network Security Total Cost of Ownership.....	1
Evolving Internet Requirements	3
Current Security Risks.....	3
Assessing The Risks	6
Security Solutions	7
Issues With Legacy Network Security Architectures	8
Next Generation Solutions: The Integrated Network Security Platform	9
Astaro Security Linux	10
Leveraging Open Source Software	11
Conclusions.....	12
Further reading.....	12
Appendix A: Best-of-breed Security Applications Leveraged By Astaro	13
Appendix B: References	14

Evolving Internet Requirements

Internet access has become vital to the normal operations of virtually every organization. In the 2003 UCLA Internet Report over 90% of all respondents rated the Internet as a moderate to extremely important source of information. Studies show it has enabled organizations to:

- Greatly facilitate collaboration between employees, partners, suppliers and clients through vehicles such as email, file sharing and web conferences
- Rapidly access information through on-line searching, databases and e-training
- Inexpensively provide services to outside organizations through web sites, email distribution and on-line commerce applications

In summary, the Internet is used widely across most organizations, enabling them to increase productivity and the quality of services, while decreasing costs.

With this widespread adoption has come a change in user and management attitudes. Internet access is no longer a luxury. It is a mandatory business requirement. Unencumbered, transparent access is expected at all levels in the organization on a non-stop basis.

Current Security Risks

Unfortunately the Internet has a dark side too. Just as it provides transparent access to numerous external resources for an organization, it can also provide external parties, not all of who have good intentions, relatively easy access to the organization's internal computers and information. All types businesses are at risk. On a whim, in 2002 a 22-year old hacker scanned the New York Times' Internet gateways, and was easily able to access numerous databases providing personal information on sources, employees and customers. Even highly sophisticated businesses like computer game maker Valve Software have experienced Internet breaches. Valve has had information and source code for pending product releases posted on the Internet, a breach that may have severe financial impact on Valve.

The diversity of methods used to malevolently access or attack organizations' computers through the Internet is truly stunning. On top of this, inappropriate internal use of the Internet is also turning out to be a big issue. The following are some of the forms of abuse reported by IT managers to be of greatest concern:

Network Security Facts:

The average cost of an external security breach in 2002: \$226,000.

The average cost of a virus infection in 2002: \$81,000.

The average cost of a DoS attack in 2002: \$297,000.

Type of Attack	Description	Economic Implication
Hackers	Hackers, or skilled programmers who find challenge in breaking into other people's computer systems, were traditionally the greatest threat to organizations' computer security. While they still pose a threat, widespread deployment of countermeasures such as firewalls has caused other forms of more sophisticated malicious attacks to emerge. (Note: Although the term hacker can also mean one who is proficient at using a computer for legitimate needs, we do not use that meaning in this paper.)	After breaking into a system a hacker may steal, delete or alter valuable data, programs or identities.
Malware	Malware (viruses, worms, etc.) are pieces of disguised code that are typically designed to cause an undesirable event, such as altering existing computer files or making the computer inoperable. They can be transmitted by disk, email or other communications vehicles. Because email usage is so prevalent, and traditional security systems remain vulnerable to viruses, viruses are now one of the major security concerns of IT managers. 86% if all infections stem from email attachments.	The cost of lost productivity, restoring damaged files and cleaning up viruses was a staggering \$13.2 billion worldwide in 2001.
Spam	Unsolicited commercial email messages (spam) are not created with the same malicious intent as threats like viruses, but are now having a negative economic impact on the same order of magnitude.	Spam clogs networks, hogs disk space, and wastes countless hours of users' time reading and dealing with the messages. Estimated cost to U.S. and European businesses in 2002 was \$8.9 and \$2.5 billion respectively.
Denial of Service (DoS)	A DoS attack is one in which the perpetrator deprives an organization of the use of a network resource (such as the email system or web site) by sending network traffic that exploits a weakness in the receiving system (for example, an inability to deal with a large number of email connection requests in a short time). The more sophisticated Distributed DoS attack utilizes a common exploit to first penetrate numerous widely dispersed systems, and then launch the attack from those systems, making it harder to detect and block.	Since organizations depend upon these services to conduct business, the impact on revenues and productivity can be quite substantial.



Reducing Network Security Total Cost Of Ownership

Astaro www.astaro.com info@astaro.com
Pfinztalstrasse 90, 76227 Karlsruhe, Germany
67 S. Bedford Street #400W, Burlington MA, 01801 USA

Type of Attack	Description	Economic Implication
Inappropriate Web Usage	Because Internet usage cannot be casually monitored, some individuals use it to access inappropriate material (pornography, hate material, copyrighted audio files) and conduct inappropriate activities (excessive personal business, etc.).	Given the large number of employees with Internet access, clearly there are potential productivity issues associated with unrestricted usage. A growing concern is associated legal issues. Allowing the downloading of inappropriate material without controls can result in expensive lawsuits for a hostile workplace environment and copyright violations, for example.
Insider Attacks	Although most attacks originate from outside the organization, internal attacks are not infrequent, especially those related to theft or destruction of proprietary information. Roughly half such attacks originate internally. Disgruntled employees, as well as those seeking personal financial gain have used their insider status to access, and sell or destroy valuable company information.	Insider attacks can be more harmful than attacks by hackers due to the knowledge the perpetrator has about the location and use of valuable data.

Assessing The Risks

Clearly the Internet presents a variety of real threats to those connecting to it. The first question facing any organization with limited resources is: "Which, if any of these threats is substantial enough to justify spending money and management attention on?"

As a starting point, ponder the data from the annual survey conducted by the FBI and Computer Security Institute. Results show that roughly 80% of organizations now site the Internet as a source of *frequent* attacks, with the percentage experiencing *frequent* attacks growing steadily.

Unfortunately not only is the volume of attacks increasing, but also the variety and sophistication of attacks is on the rise. A recent survey of IT leaders shows that the top five forms of *breaches* (successful attacks) have been experienced by 63% to 82% of IT leaders surveyed in the last year! The statistics for unintentionally harmful threats are equally substantial. Consider:

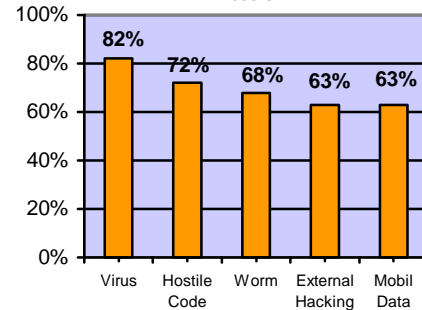
- 46% of all email today is spam
- In 2002, 60% of surveyed employees with Internet access reported they use the web to conduct personal business, while 57% reported they use email for personal transactions.

Clearly this data shows that every organization, no matter what its size, has reason to believe that it will be subject to a significant variety of Internet-based threats. The economic impact of such threats is more difficult to quantify because they vary depending upon the type of organization (business, non-profit, etc.), the nature of the breach, salaries and so forth. But some of the general statistics available do provide an idea of the magnitude of the impact:

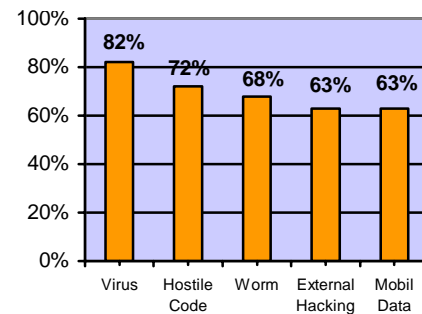
- The average cost of an external security breach was reported to be \$226,000 in 2002 according to the FBI/CSI survey of 503 organizations.
- DoS attacks cost \$297,000 on average.
- The average cost of a serious virus infection (25 or more PC's) was reported to be \$81,000 in the 2002 ICSA survey.
- Damages in lawsuits for work hostile environments have ranged from \$25,000 to multiple millions of dollars.

Clearly the economic and organizational impacts are high enough to not only warrant, but to demand investment in protective measures for each of the major threats.

% of Organizations Citing Internet As Frequent Point Of Attack



% Of IT Leaders Experiencing Security Breaches By Type In The Last Year



Security Solutions

Just as different forms of attack emerged separately over time, so to have a variety of corresponding point security solutions. Major solutions currently being deployed include:

Security Solution	Description
Firewall	<p>A device that is placed at the point where the Internet enters a facility, controlling network traffic for security purposes. It examines all inbound and outbound traffic; permitting only traffic meeting predetermined criteria to pass. This allows unsolicited traffic from hackers to be blocked (including DoS attacks), while maintaining transparent Internet access for employees and customers. Firewalls that incorporate application proxies can block some forms of attack disguised as legitimate traffic and perform other security and inspection functions. To minimize internal threats firewalls can also be used to segment an internal network.</p>
Virus (Malware) Protection	<p>A form of computer program that searches targeted software, such as email and attachments, for known or potential malware such as viruses. Two forms of protection are commonly available:</p> <ol style="list-style-type: none"> 1. Host-based scanners: Installed on every computer in the organization, including mail servers and desktop PC's, they scan each file received or sent from that system. 2. Gateway-based scanners: These reside on a single computer (or gateway appliance) that sits at the Internet's point of entry to an organization, scanning all inbound and outbound email and attachments. <p>Ideally an organization should install both forms of protection to add an extra layer of security. However, if budgets are limited, the perimeter approach is easier to administer, more secure and more cost effective.</p>
Spam Protection	<p>One or more electronic filters, each using a particular detection technique, which together work to identify and block spam. Common techniques include:</p> <ul style="list-style-type: none"> • Real-time blackhole list: Utilize one of the publicly available lists constantly updated with the addresses of known spammers to block messages. List accessed via Internet by the filter. • Sender verification: Spam protection program that verifies sender's legitimacy by contacting the transmitting server or using DNS for verification. • Heuristics: Program that rates incoming mail on the match with common spam characteristics, and allows a threshold to be set, above which the email is spam. <p>Again, spam protection can be deployed on each desktop, or at the perimeter. Perimeter protection is more cost effective from an administrative and cost perspective.</p>
Surf Protection (URL Filtering)	<p>A computer program which typically:</p> <ol style="list-style-type: none"> 1. Monitors web traffic to allow analysis of utilization. 2. Places web pages into categories meaningful for blocking (e.g. pornography sites, gambling sites, etc.). 3. Provides a means of establishing rules for blocking categories. 4. Blocks and notifies users when they attempt to access a prohibited page. Logs blocking for management action. <p>Also called Surf Protection, web blocking or content filtering.</p>
Wireless Protection	<p>A device that interfaces with wireless computers, providing encryption of traffic and authentication of the wireless users, in addition to the firewall functions described above (similar to VPN). This protects against the additional hazards</p>

Security Solution	Description
VPN (Virtual Private Networking)	<p>inherent in wireless communication: interception of wireless data by 3rd parties, and backdoor access to network resources through the wireless network.</p> <p>Computer software residing at both ends of a remote communications connection that enables the establishment of secure virtual tunnels through a shared public infrastructure such as the Internet. VPN's provide the security benefits of private lines with the cost structure of public networks.</p>

Issues With Legacy Network Security Architectures

The table above illustrates the nature of today's situation. Information Security Magazine's 2003 Buyers Guide features 1,900 products from 850 vendors in 66 security categories!

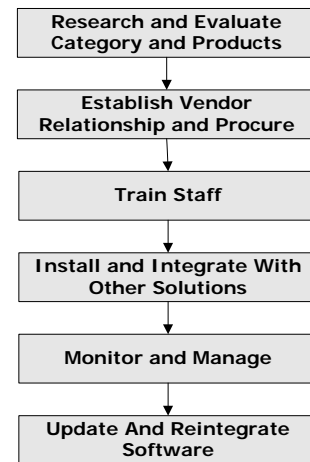
Piecing together an effective security solution from these components is not trivial. First of all, each component requires investment not only in terms of software and hardware purchase costs, but also in terms of upfront and on-going labor. Unique installation requirements, configuration parameters, user interface and management needs demand separate training and administrative procedures. With IT staffs stretched thin managing existing applications, adding another piece of software and hardware requiring proficiency is problematic, even if the budget is available.

Integration is another problem area. Connecting various security point products such as virus protection, firewall, spam and web filtering creates the opportunity for security gaps. The potential for introducing configuration issues and increased latency is obvious.

The overall quality of the security solution must also be considered. Security is only as strong as it's weakest link. With a wide variety of point solutions required to form an effective defense, and 1,900 products to choose from, understanding and selecting the appropriate components is a burden for most organizations.

In short, the current approach of weaving together a security shield from a variety of different point products is especially problematic for organizations with limited staffs and budgets.

Major Lifecycle Costs Of A Security Solution



Next Generation Solutions: The Integrated Network Security Platform

To overcome these issues, and meet the needs of today's resource constrained organization, a security solution should have the following attributes:

- Include protection from all the most common threats by providing firewall, virus protection, URL filtering, VPN, wireless and spam protection functionality at a minimum.
- Provide world-class solutions to each threat. Security is only as strong as the weakest link.
- Run on a single hardware platform, which can be upgraded as traffic volume increases without having to scrap the investment in the existing solution.
- Install all components, including a security hardened operating system, from a single CD. Alternatively it should come pre-installed on the hardware.
- Share configuration information among all components to reduce administrative effort and errors.
- Provide a common management interface for all security functions, and further minimize administrative labor and training needs by using a point-and-click paradigm.
- Be designed as a software platform, so as new threats arise they can be integrated without requiring the existing solution be scrapped.
- Provide automatic updates of all security and operating system functionality through a single Internet source, minimizing operating costs and security gaps.

There is broad recognition of these needs from analysts such as Gartner and Yankee Group, as well as many in the vendor community. However significant obstacles exist for existing solution vendors in meeting these needs:

- Unless a product is specifically designed as an integrated security platform, with thought given to how different security applications are integrated at the user interface, configuration and run-time levels, it is quite difficult to "add" an additional security function in an effective, seamless manner.
- Products tied to specific hardware platforms are impeded by the fact that new software functions alter the processing, memory and storage requirements of the hardware, typically requiring a new platform.
- No single vendor has the resources or the specialized skills to provide world-class solutions to the variety of threats to be addressed.

"Gartner believes that enterprises are moving toward an integrated network security platform approach ... Tighter integration and common management across security solutions will provide customers improved attack blocking and lowering total cost of ownership."

-Richard Stiennon, Research Director, Gartner

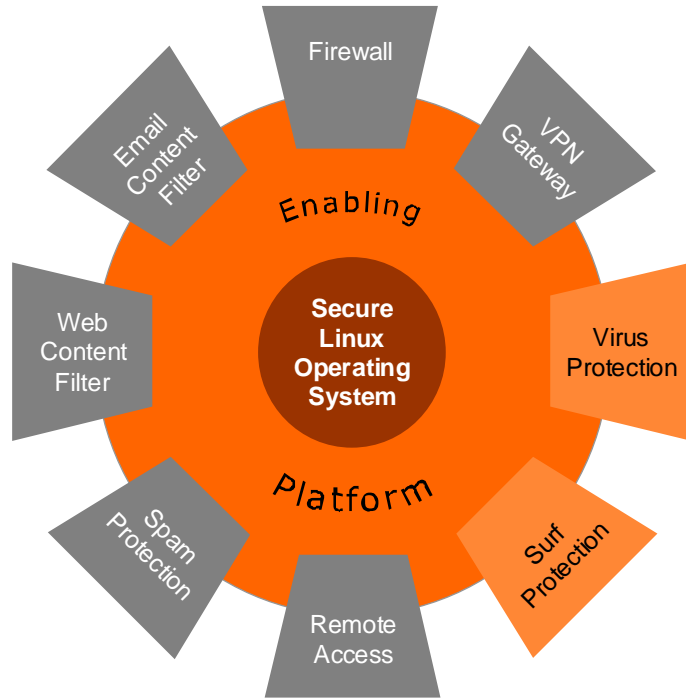
The problem requires a new approach.

Astaro Security Linux

Recognizing this need, Astaro set out to build a comprehensive, affordable network security product designed specifically to meet the requirements of resource-constrained organizations.

Core to accomplishing this was development of a next-generation software architecture that allows best-of-breed security applications to be integrated into a single easy-to-use environment. The architecture includes:

- An enabling platform capable of integrating diverse applications, including those not specifically designed for Astaro.
- Common system services for all application modules, such as high availability, status monitoring, and so forth.
- WebAdmin, an intuitive browser-based point-and-click user interface that manages all the applications in an integrated manner.
- For larger organizations with multiple devices, an interface to a centralized configuration manager. Astaro Configuration Manager supports the graphical design of security policies for all Astaro firewall and VPN devices from a single central console, as well as the automatic generation and upload of corresponding configurations.
- Up2Date, a common service for managing automatic software updates to all modules using a secure Internet connection.



Astaro Security Linux Architecture

Astaro’s solution, known as Astaro Security Linux, was built on top of, and includes, a security-hardened version of Linux. As a result, there is no need to integrate or customize an operating system.

Leveraging Open Source Software

With respect to security applications, the flexibility of the Astaro architecture has enabled the company to focus on finding best-of-breed solutions for the major threats facing users. A summary of these applications is included in Appendix A.

Many come from the open source community, which develops some of the most secure, sophisticated security applications available. Examples include firewall, spam protection and VPN gateway functionality. Because the source code for the applications is openly available, it is subject to the scrutiny of numerous developers, who swiftly contribute suggestions to any issues or needs uncovered. In contrast, the proprietary security applications marketed today are developed by a small number of developers, and are not subject to significant scrutiny. This is the reason some of the most demanding security environments in the world, such as the U.S. military, use open source software.

Another benefit to open source software is cost of ownership. Because Astaro does not incur development or royalty expense for these modules, the cost of the solution when compared to organizations developing proprietary software to meet these same needs is dramatically lower. Similarly, during the entire lifecycle of the solution, the open source community continues to enhance and evolve the applications. Astaro allows users to leverage this on-going development stream while relieving them of the need to track, test, integrate and deploy the updates. Astaro's Up2Date service automatically delivers tested and integrated updates for all software components via the Internet.

Astaro uses open source software when proven, secure, world-class applications are available. For some needs, such as virus-protection and URL filtering, open source is not currently an appropriate solution. In these cases Astaro has sought out the best commercially available solutions:

- Virus protection from Kaspersky Lab: Kaspersky has a staff of 250 virus protection specialists who constantly monitor the Internet for emerging threats, delivering new updates hourly. The Kaspersky engine uses a combination of signature, heuristic and emulation techniques that have consistently delivered market-leading results in independent tests of detection accuracy.
- URL filtering from Cobion: Cobion's massive farm of over 1,000 servers constantly crawls the Internet, and using a combination of keyword, intelligent text classification, image analysis and OCR techniques classifies web pages into 58 categories. Cobion technology has also delivered market-leading results in terms of accuracy, and does so in 11 different languages.

Astaro's approach has furnished a solution that is not only comprehensive, but delivers outstanding security.

Conclusions

The Internet is an indispensable element of conducting business. Its popularity has attracted an increasing number of undesirable elements, who are launching increasingly sophisticated and varied attacks ever more frequently. To cope with the hostile environment users need a comprehensive security shield. Organizations with limited staffs and budgets are not in a position to fabricate this shield from a variety of products from different vendors. Nor is such an approach desirable from a security or management perspective.

Astaro provides an affordable, easy-to-use, comprehensive security solution with best-of-breed applications for needs including:

- Virtual Private Networking
- Firewalling
- Virus protection
- Content filtering
- Spam protection
- Wireless protection
- Traffic shaping

The solution is available as a software application for installation on standard PC hardware, or pre-installed on a hardware appliance. Acclaimed for its power, ease-of-use and affordability by SC Magazine, LinuxWorld, InfoWorld, LinuxJournal and other independent reviewers, Astaro Security Linux is designed to evolve with the rapidly changing security requirements of its customers.

Further reading

InfoWorld Magazine reviews Astaro Security Linux and reports "the most polished and easy to use Web-based management system we've seen to date." ([Read the whole article as PDF](#))

"A stylish-looking appliance that addresses the major internet-related security concerns of the small or medium business," says SC Magazine. ([Read the SC Magazine article as PDF](#))

Astaro named winner of the [product excellence award](#) at LinuxWorld.

A free 30-day fully-featured evaluation version of Astaro Security Linux can be downloaded at <http://astaro.com/php/download.php?lang=gb>



Appendix A: Best-of-breed Security Applications Leveraged By Astaro

In order to deliver a comprehensive, world-class security solution, Astaro selects and seamlessly integrates outstanding security applications whenever possible. This table provides a partial listing of the 60+ security applications leveraged by Astaro Security Linux.

Application	Source
Packet Filter	Open source: Netfilter
Virtual Private Networking	Open source: Super FreeS/WAN/PPTPd
Proxies	Open source: Squid, Bind, Exim, DHCPd
Content Filter	Open source: Exiscan, ActiveXFilter
URL Filter	Cobion Corporation
Spam Filter	Open source: Spam Assassin
HTTP Server	Open source: Apache
Traffic Shaping	Open source: Linux QoS
Management Agent	Open source: UCD-SNMP
Secure Sockets	Open source: OpenSSL, OpenSSH
Virus Protection	Kaspersky Lab
Reporting	Open source: Mrtg, syslog, WebReports
Astaro Configuration Manager	Solsoft Corporation

Appendix B: References

1. Surveying The Digital Future: The UCLA Internet Report, UCLA Center For Communications Policy, 2003
2. Countering The Greatest Fears, Information World, 8/26/02
3. Computer Security Issues and Trends, Computer Security Institute, Volume 8/Number 1
4. Information Security, News and Analysis – Net Intrusions, 7/1/03a
5. Web Connection: The Global Virus Impact, Electronic Commerce World, 4/1/02
6. Hitting Spammers Where It Hurts, Business Week, 5/19/03
7. ICSA Labs 8th Annual Computer Virus Prevalence Survey, ICSA, 2003