An Overview of
Computer Network Security
Products & Devices

Robert Demaine

Version 1.3

I. Summary

Every network administrator is faced with the daunting task of securing their computer network and networked workstations. They are securing their systems from potential inside, or outside attackers. There are several general methods a network administrator can use. These methods include firewalls, system hardening, host or network based intrusion detection (H-IDS, or N-IDS respectively), and vulnerability assessment. Familiarization with the different products and services available under these categories is the first step to implementing a good virtual security plan.

There are a number of commercially available products aimed at securing computer networks. When a using a layered defense, there is a greater chance of mitigating or blocking an attacker from gaining access to a computer network. There are many more products that are available than those discussed in this overview. Every network is different, thus the virtual security of every network is going to be unique.

II. Firewalls

Putting a firewall in place is one strategy that most network administrators use to protect their network. The idea behind a firewall is to secure all points that connect to other networks, with a mechanism to regulate network traffic. Used effectively, a user will log into the firewall "device" (This could be either a hardware or software based firewall) to gain access to resources outside the network, such as the Internet. Firewalls can be configured to regulate virtually all network traffic passing through it. Firewalls should not be the only defense mechanism to protect a network, because firewalls tend to give network administrators a false sense of security, about their network security.

SonicWall has a line of firewall hardware devices available for the SOHO (Small Office/Home Office) and enterprise networks. The SonicWall SOHO is available for small networks, and the SonicWall Pro 300 is available for enterprise networks. Their line of devices offer different levels of security, and complexity based on the version of the device. [1] The SonicWall series of firewalls can be configured through a browser interface. SonicWall line of devices include 3DES encryption (Data Encryption Standard, this is used 3 times to encrypt and re-encrypt data), are certified by the ICSA (International Computer Security Association), employ stateful packet filtering and interface seamlessly with other products or services offered by SonicWall. [2] The SonicWall firewall line is designed to be one part of an integrated system that can be used to secure a computer network.[3]

By using a piece of hardware for firewall functions, an administrator can eliminate the need for a host operating system that would be subject to attacks, or crashing. Hardware can eliminates bottlenecks by running at near network speeds, as opposed to other filters that will slow the flow of network traffic. [4] The cost for the SOHO version is around 400$, and the enterprise version around 2,000$.[5] SonicWall offers other products and services aimed at protecting computer systems. These products and devices are designed to work together to provide a more complete network security.

Information about SonicWall firewall devices, or services go to http://www.SonicWall.com.

By using a separate device to regulate traffic, a network administrator can offload these functions from their router. Offloading these functions from a router allows routers to route traffic, and the firewall to regulate traffic. One advantage of using a central firewall, like this one, is that it is placed in a central location, eliminating the need for installing personal firewalls on network workstations.

Symantec Enterprise Firewall 7.0 is a software solution that runs on Windows NT or Solaris systems. It supports AES encryption (Advanced Encryption Standard), load balancing, full inspection of all network traffic, and does not slow the flow of approved network traffic.[6] Like SonicWall it can be used in conjunction with other Symantec products such as their enterprise anti-virus, and VPN software. Symantec Enterprise Firewall 7 can interface with existing network authentication systems like: Radius, LDAP (Lightweight Directory Access Protocol), Defender, Digital Certificates and Windows NT (New Technology) domain authentication. Information and cost are not readably available for Enterprise Firewall 7. [7]

This form of a software based firewall is subject to attacks aimed at the system it resides on. If the host computer were compromised, the firewall would go down. An advantage to Symantec's Enterprise firewall is that it can be interfaced with other existing authentication systems, making it relatively easy to implement. Information about Symantec products can be found at www.symantec.com.

Symantec offers a desktop firewall. This firewall runs in the background, regulating network communications to and from the host computer. Traffic is regulated based on a set of rules. The rules can be setup in two ways. The first way is by using the default rules that are created upon installation. The software automatically tailors rules for each computer it is installed on, reducing the overall complexity of a default install. This automatic integration allows the firewall to be installed with ease. The second way to create rules is through the software. Policies can be customized by the users. Administrators can change, modify, add and delete rules based on what they feel is necessary. The user can control access to files on their system, this allows them to safely share some files while allowing the rest of their data to remain private. The system will alert the user when a potential security threat is detected. Many companies are setting up VPN's for remote users; Symantec desktop firewall is vendor neutral and will easily integrate itself with most popular VPN devices or services for an increased level of network security.[8]

Desktop firewalls can be used on computers connecting to a network over an Internet VPN. Symantec Desktop Firewall is available for 20-30$ per workstation, and is relatively easy to setup. Installation of this firewall must be done at the workstation, or through 3rd party software designed to "push" software to the desktop. Information about this product can be located at www.symantec.com

Cloudshield is a company that created a hardware appliance aimed at firewalling and intrusion detection for large enterprise, government or ISP (Internet Service Provider) networks. They are calling their hardware device a "packet processor". The packet processor was designed to be placed between the OC-48 optical line (Optical Carrier) and edge routers or switches. The packet processor is able to work at line speed, so it does not create a network bottleneck. The packet processor can be used as a firewall, VPN filter, intrusion detection device, and provide overall network security. Cloudshield claims that the device analyzes packets on layers 2 through 7 (Data link to Application layer).[9]

The Cloudshield packet processor will allow network administrators to offload packet processing functions from routers or switches, to this device. This will enable administrators of enormously large networks to reduce the overall number of network devices that are used specifically to process packets. The packet processor works by using parallel processing techniques to separate different functions the processor looks at. If a router were to do the same thing as this packet processor, it would take several terabytes of memory.[10]

Hardware can process data much faster than software can. Allowing a hardware device to take raw input from a network connection, process the data, and compare it to a set of rules, a network administrator can reduce the number of other filtering devices. The reduction in networking equipment has the potential to reduce the amount of electricity their overall networking equipment uses. The list price is unavailable for this particular product. If Cloudshield can produce this kind of a product for enterprise networks, imagine what they could do to help medium to small networks in the future. Information about Cloudshield's packet processor can be found at www.cloudshield.com.

III. System Hardening

Network-1 CyberWall PLUS products can be used to secure individual Microsoft Windows NT, and 2000 server and workstation systems (More information can be located at www.network-1.com). CyberWall PLUS regulates traffic that communicates with the host system. When the software is installed, it integrates itself on the kernel level and protects the operating system from processing harmful data. CyberWall PLUS combines packet filtering, stateful packet inspection, and intrusion protection. [11]

CyberWall PLUS works at the lowest possible system level to monitor incoming and outgoing Ethernet frames. This helps to regulate the network protocols communicating to and from the host system, effectively blocking any harmful data before the kernel can process it. CyberWall PLUS can use pre-defined policies or user defined policies. Security policies are applied to all packets passing through the computer. It protects against IP (Internet Protocol) spoofing, oversized packets, and other types of attacks. A central management console is used to monitor and modify policies in real time. This console also creates reports based on the logs that are kept.[12]

The CyberWall PLUS suite contains "intruder detection". This feature alerts administrators of suspicious activities by monitoring network conversations. The software can be setup to alert administrators in many forms. There are local alerts, paging alerts, direct action and e-mail alerts. Alerts or responses can be configured for specific events, in any of those forms.[13]

There are several versions of CyberWall PLUS for different uses. CyberWall PLUS-SV is intended for network servers, CyberWall PLUS-WS is for workstations, CyberWall PLUS-IP is a traditional IP firewall, CyberWall PLUS-CM is the central management console, and CyberWall PLUS-AP can be used as a transparent bridge to monitor multiple protocols.[14]

The CyberWall PLUS suite of utilities can be useful to watch servers in a DMZ (Demilitarized Zone), where there is access to servers from the Internet. In a DMZ a network segment that is generally less secure (By design, or by ignorance), than network segments inside the perimeter. Usually within the network perimeter, there are more intrusion detection & prevention systems. The CyberWall PLUS line of utilities can be helpful inside a network, if a server contains sensitive information. It can be used to increase security on these systems if inside attacks are a possibility. CyberWall PLUS is an effective addition to any virtual security system. Network 1 has information about CyberWall PLUS published on their website, www.network-1.com.

IV. Intrusion Detection

The Psionic Tri-sentry suite is composed of three individual parts. These utilities are: a port scan detector, a host based component and log analyzer. This suite of applications is designed to solely run on UNIX based systems. The system components work in real time to monitor and block desired or undesired traffic on a network or to a network host.[15]

Psionic Port Sentry monitors a network for port probes, and then takes action to block or drop them. When a port probe is detected, Port Sentry directs the probe into a "black hole" and drops the connection. The program can monitor TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) port probes on a variety of sockets using the same daemon to detect them, eliminating the need for more than one instance of the program to run. On Linux systems it can detect half open ports, "stealth" scans of a system, and react to the stimuli by using TCP wrappers. All activity is logged and entered into a database. Logging helps to identify false positives, repeat attacks and/or attackers.[16]

Psionic Host sentry logs user activity between the time a user logs in and when they log out. The program tracks what programs were run, by a user while they were logged on. When it is first installed, the software collects data on the 'user habits' logged into the server. It does this to create a baseline for what is "normal" network traffic. When it is first installed, it will alert the administrator about everything that is taking place on the network. Once the system has a baseline, it will detect and report any 'unusual' activities and react to it. The reaction is based on what the administrator has programmed it to do.[17]

Psionic log sentry monitors your system logs and alerts administrators of security violations periodically. The program can log changes to any system log file, operating system violations and strange events. Used in conjunction with a network based IDS, and the complete Tri-sentry suite, this product will is an effective tool that can be added to a layered defense strategy. [18]

UNIX based systems are used on many networks, Psionic has created a free product specifically designed for UNIX environments. The logs that are created allow an administrator to determine the events that led up to a network security breach. Once they know how an attacker got in, they can close the security hole in the system. By nature, most detection systems are reactive, meaning that they rely on a previous attack in order to block future attacks of the same nature. The Tri-Sentry suite logs attacks, alerts administrators to security violations, and stops an attack. The logs can be used as a tool to determine what needs to be done to mitigate a similar attack in the future. Psionic Tri-Sentry can be downloaded at www.psionic.com, and is free to use.

Okena produces what they call an intrusion prevention suite of utilities. The utilities include: Okena StormWatch, Okena StormFront and will include StormTrack. Okena uses a behavior-based engine to detect anomalies, as opposed to using fingerprinting or signatures to detect them. By using a behavior engine, as opposed to a signature database, the software can protect against unknown attacks.[19] This behavior engine makes Okena a versatile tool for blocking unknown, future attacks.

The system currently has 3 key components. The first component is the central management console, which is used for creating policies, gathering information from the agents, and the profiling of programs. The console costs roughly 2,000$ and manages 2,500 agents. Before you can "turn on" the prevention system, you must create a policy for the operating system files, and any applications that need to be accessed. Okena provides a few policies that define popular Microsoft operating systems, and other popular software.[20]

StormWatch is the second component, which is the host portion of this package. StormWatch resides on the host workstation or server (This component is the intelligent agent). StormWatch utilizes the policies created in the management console to stop unauthorized processes. If a program does not fit into any of the policies, then the process is stopped "dead". The system was able to stop Nimda, Code red I, Code red II, Sircam and other viruses before they had a chance to infect protected systems. [21]

StormFront is the third part of the suite. To enable the use of custom software, an administrator must use StormFront to "profile" a program. Profiling allows for appropriate policies to be created.[22] StormFront is used to gather information about the target program and the files associated with it. Once this step is completed an administrator can create an effective policy for the target program. StormWatch stops any process, if it lacks an active policy, which is why it is necessary to profile a program and create a policy for it.

StormTrack is still being developed, and Okena claims that it will be able to "StormTrack uses the StormWatch agent to rapidly identify unprotected components of the IT infrastructure and easily close exposures using the other StormSystem components, automatically determining whether to add a pre-existing security policy from StormWatch or create a new and custom policy with StormFront." This procedure would use the already agents to gather data, analyzes the data to help put into place a new security policy.[23]

According to an e-mail I received from George Milliken of Farm-9, a security consulting company, Okena StormSystem is a fairly inexpensive intrusion detection and prevention system. It is effective because it is not based on signatures, but rather policies thus it will (and has) prevent new attacks from occurring. He states that defining the policy "... is probably the biggest issue. However they have a new tool, StormFront, that makes the process much easier." He also says that even if the system administrator is behind in service packs, the intrusion system still works. This is largely due to the fact that it is a policy, rather than signature based system.

The management console costs 2,000 $, the server agent costs 800$, and the workstation agents cost 50$, each. It should be noted that the management console can only manage 2,500 agents.[24] Perry Tsacoumis, technical director for a research and development project at government contractor Northrop Grumman IT/Logicon, has only one complaint about Okena StormSystem. His complaint is that Okena is "only available for Windows platforms".[25]

Based on its track record with Code Red I & II, I would judge StormSystem a very effective host IDS solution. The system effectively "locks down" a workstation or server. This means that software that is run on computers and over the network can be regulated. This can allow for Okena to double as a control mechanism for prohibiting the use of unlicensed or unapproved applications. This in itself can prevent network attacks by prohibiting the intentional or unintentional installation of back doors. Like any security system this makes an excellent addition to network a more complete virtual security system. Information about Okena StormSystem can be found on Okena's web site, at www.okena.com.

Symantec Intruder Alert is a host based IDS system that reports to a main management console. This system is able to monitor networked computers in real time. Intruder alert allows an administrator to create a set of highly granular policies for detecting suspicious activity, enable the enforcement of security policies, and allows for the administrator to respond to security breeches. The administrator can specify a range of responses to different stimuli, these alerts range from an on screen alert to direct action. The central console allows for the creation, distribution and update of security policies. The central console also collects information and reports it to the administrator in easy to read reports.[26]

Symantec intruder alert will run on NT, commercial versions of UNIX, and Novell Netware. It uses agents, managers and a central console. Each agent resides on a host that is monitored. The management computers are used to control up to 100 agents that report to the central console. The central console can monitor up to 10 managers or 1,000 computers. The ways agents are run on the host are the following forms: agents are run as a daemon in UNIX, as a service in NT, and an NLM (NetWare Loadable Module) in Netware. The manager runs as a daemon in UNIX or a service in Windows, and cannot be run in Novell.[27]

Intruder Alert solely monitors TCP/IP communications. There are over 400 different attack signatures with more added to the dictionary each year and custom policies can be created via the central management console. From the central control panel, the software and policies are updated from an explorer-like environment console. Intruder Alert monitors 8 key Windows files every 30 seconds and other files every 8 hours. An administrator can set the timing, and the files that they wish to monitor. In an NT system, application, security and sublogs are monitored, in UNIX syslog, wtmp, btmp, C2 logs are monitored and in NetWare, callbacks are monitored. All of these functions can be manually added, edited and deleted.[28]

Data collected by Intruder Alert can be used in forensic investigations. All the data collected is compiled and stored in an encrypted file on the management station, communication to the log is also encrypted and authenticated. When setting up the alert options, there are 14 alerts that fall under the categories of "notify", "recording", and "reacting". All 14 options can be manually set by the administrator.[29]

Symantec Intruder Alert requires planning before it is setup. Each agent and manager set must be planned for, which can make the installation process complex. Administrators can use 3rd party software to install Intruder Alert over a network, or visit each target computer. This can add to the time it takes to implement the system. Intruder Alert is signature based, which means that it cannot protect from unknown attacks. Symantec releases updates sporadically, making it difficult to know if a network is truly secured. (Previous release dates are found at http://securityresponse.symantec.com/avcenter/security/Content/Product/Product_IA.html.) As a part of a layered defense strategy, Intruder Alert would provide some protection over a TCP/IP network against known attack patterns. The cost of this system is difficult to locate.

V. Vulnerability Assessment

Security Analyst is an agentless host vulnerability assessment and analysis package. Security audits are becoming increasingly important to businesses to find weak points in their networks, before an intruder does. Security Analyst is designed to audit Windows and Novell NetWare (Version 3 and up). The software is designed to take a companies security policy and compare it to what is currently being implanted. It mainly checks user accounts to see if the established policy is being implemented. [30]

Security Analyst requires administrative or supervisory rights on the domain or NDS. The software runs on a Windows NT or 2000 Professional workstation. It tests 6 different security criteria: Password strength, access control, user account restrictions, system monitoring, data integrity, and data confidentiality. [31] The account restrictions test verifies the login restrictions implemented, are what exist in the directory (NDS or Domain). The password strength test checks passwords for their complexity, to be sure that they cannot be easily compromised. The access control test reports what system resources are available to each user. The system monitoring test checks the logging features on each server, to be sure that the proper information is being logged. The data integrity check looks at the how data loss prevention is handled. Finally the data confidentiality test looks at how secure data is while it is in transit and stored on the network servers. The software uses adaptable, industry "best practices" policy templates. These templates can be customized based on the organization's security policy. [32]

Security Analyst runs on a single desktop workstation connected to the network. On the network it is auditing, the workstation requires administrative or supervisory rights. The software requires the workstation to be a Pentium 2, with 1 gigabyte of disk space, and 128 megabytes of memory. Other requirements are the ability to have 1024 x 768 screen resolution, data access control needs to be setup in ODBC, and Adobe Acrobat Reader is required to read the reports. One major setback is that Security Analyst cannot audit the "new" Windows 2000 AD (Active Directory) service.[33]

Security Analyst is a good way to regularly test user accounts for deviation from an organization's security policies. The software is able to run on a workstation, which leaves server resources free to do other tasks. One problem is that there are companies that are planning to, or have implemented Active directory. Currently Security Analyst cannot test Active Directory. It would be beneficial for future revisions of Security Analyst to include the ability to scan an AD network.

Being able to test the level of security on a network and compare it to company policy, can be a beneficial tool to help rectify any inconsistencies there are among user accounts and user account policies. Security Analyst is a practical way to periodically check for security infractions on Windows and NetWare networks. The cost associated with Security Analyst is about 600$ per directory (Domain or NDS).[34] Further information about Security Analyst can be found at www.intrusion.com.

Symantec Enterprise Security Manager 5.5 is a policy based assessment and management tool. Enterprise Manager requires the administrator to setup agents on the host systems in order to collect information then report it to a central manager (It seems that Symantec likes central management and 3-tiered systems.). It supports Windows, UNIX, Linux, and open VMS systems making it more versatile than Security Analyst. The agents can be remotely installed, silently installed or locally installed on a host system, from CD or network distribution software. It is preconfigured with industry "best practice" security settings. These policies can be easily modified to match an organization's security policy. It also can give administrators a fine grain control over the security policies that are in effect.[35]

Each host that is monitored requires an agent to be installed on it. Each agent is in turn controlled by a management station. The management station is installed on one system and collects data from the host based agents. The managers instruct the agents to send their data for the administrator to view at the central console. The data is stored in a local database until the manager accesses it, it is then stored on the manager until the administrator views it at the console. The console collects, compiles and reports the data for the administrator. This is a tool that is very effective in both auditing security policy, and implementing detailed security policies.[36]

Symantec's Enterprise Security Manager is easily scaleable to larger networks, because it uses a 3-tier system of agents, managers and consoles. Deployment of this system takes a lot of planning for the system to be effective. The software can be deployed through network distribution software, and once deployed can be updated though the central control panel. The cost of this system is roughly 1,500$.[37](More information can be found at www.symantec.com

Network computing does a vulnerability assessment by assigning a team of people to do a "zero knowledge" attack based solely on the name of the organization. The goal of this attack is to break into a computer network, and find security holes. The team starts with the public Internet and work towards a DMZ. They attempt to find where the "firewall" stops and the network starts. Once they get in, they find a UNIX server and attempt to get super-user access by running password cracks on the password file. Next, they assume passwords are the same throughout network systems. They test this, and continue to gain access to other systems. When they get in, they put in back doors, if get detected and booted off. They find administrative machines that are trusted throughout the network, and exploit them. Administrative workstations usually contain passwords that are stored in plain text. These passwords may be for routers or other key systems. [38]

When they decide that they have gained sufficient access, they create a detailed report for the company they "attacked". This report details how they compromised the system, what types of monitoring that could have been used to detect and stop the attacks. They basically work with the IT group to secure the computer network systems.[39]

Performing this type of attack may be a good way to initially secure a system, however it is impossible to continue monitoring and evaluating the system in the same way. One would assume Network Computing would recommend a software system that they could use to continue auditing their virtual security.

The advantage of having a team of people attack a system is that software cannot detect, or anticipate any or all vulnerabilities a system may have. By having a team of people attack a system, they can quickly adapt to any mechanisms that may block or stop them. This is what a real attacker would do, so why not have Network Computing do this, instead of a malicious attacker. Detail about the methods and techniques they use are available at http://www.networkcomputing.com/815/815ws1.html.

VI. Conclusion

A layered defense using one or more of these security systems can lead to greater network security. Virtual security based on this model forces an attacker to get past a premier, a network IDS system, a host IDS, and finally other security that can be used to complement IDS systems. At some point during an attack, one or more of the systems could take direct action by blocking access to the system. A properly configured router will filter some, but not all of the malicious network traffic. A firewall should be used in conjunction with a router to filter network traffic. This allows the router to do perform basic firewall functions and complex routing functions, and the firewall to do complex firewall functions.

A determined attacker will get past any perimeter defenses, no matter how much security there is. This is what N-IDS or H-IDS systems should cover. A good IDS system will look for suspicious activity on the network, and trigger an alert or take direct action. When the IDS system fails, host based security systems should be able to take over, these are usually used as the last line of defense. If all of these virtual security systems fail, then it is time to re-evaluate the overall virtual security plan.

Using third party software to harden a system can also be an effective way of preventing unauthorized access. System hardening utilities are usually based on a set of rules for the host system. These rules should be designed to stop attacks, and try to plug any holes in the operating system. Some of these utilities can double as a host based IDS. Hardening a system is a good practice, if a host will be located in a DMZ, outside the protection of "interior" security systems. Usually attackers start in a low security network segment and work their way in to the "secure" network segment. By blocking any intruders from unauthorized access to information continued on server within a DMZ a network, information regarding the network it is attached to can be kept private.

Another option is the use of a honeypot. Honeypots can be placed on a network to lure attackers to it. There was a commercially available honeypot from Network Associates. Information about this product was unavailable from the vendor. Research suggests that this was the only commercially available honey pot that simulated a complete IP network. Honey-pots, when implemented correctly, will lure an attacker into using their tricks to gain access to the simulated system. As they attack the honey pot, all their actions are recorded. By time an attacker realizes that they have been trapped, it is usually too late.

Like snowflakes, no two networks are exactly the same. This makes it difficult to use one set of policies, rules or software to secure a networking system. Many of the products reviewed allow for the customization of their policies, to better fit the uniqueness of each network. The products that allow for close integration into each other offer stronger security, as they are more complete. The disadvantage to using one system is that, if there is an inherent weakness in a particular suite of utilities, it will could it easier for an intruder to circumvent any virtual security systems in place. A good example are Symantec products that rely on "central managers" to manage the entire system. Central management can save time, but it also offers a single point of failure within the entire system.

On a computer network there are the good guys, and there are the bad guys. At some point an attacker will attempt to gain access to a system. Where there is little or no security they will be able to get in and out, without anyone knowing about it. With a layered defense strategy, the complexity of an attack is increased, because it will take more time and resources to gain access. The longer it takes an attacker to break into a system, the chances are increased that the intruder will be detected before they have a chance to compromise with your data. Whether it is Pierre's secret recopies, or a company's enterprise sales database, your data is important and it needs to remain secure.

Works Cited

[1] "SonicWall – Products – Access Security." 2002. URL: http://www.sonicwall.com/products/access.asp. (March 16-2002).

[2] "SonicWall - Product Matrix." 2002. http://www.sonicwall.com/products/FAQ/new_faq_matrix.html. (March 16, 2002).

[3] Jarriel, Scott. *Intrusion Detection FAQ, Review of SonicWall FireWall.* URL: http://www.sans.org/newlook/resources/IDFAQ/firewall.htm. (March 16, 2002).

[4] Jarriel, Scott. *Intrusion Detection FAQ, Review of SonicWall FireWall.* URL: http://www.sans.org/newlook/resources/IDFAQ/firewall.htm. (March 16, 2002).

[5] *SonicWall Firewalls.* URL: <http://www.tribecaexpress.com/sonicwall_firewalls.htm>. (April 22, 2002).

[6] Costello, Sam. *Symantec Shores up Enterprise Firewall/VPN.* 2002. URL: http://www.computerworld.com/cwi/community/story/0,3201,NAV65-663_STO67909,00.html. (March 19, 2002).

[7] Symantec. *Symantec Enterprise Firewall 7.0.* 2002. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=47&PID=11146713&EID=0. (March 19, 2002).

[8] Help Net Security. *New Intrusion Prevention Product by Symantec.* 2000. URL: http://www.net-security.org/text/press/967471394,13603,.shtml.. (March 24, 2002).

[9] Cloudshield. *Frequently Asked Questions*. 2001. http://www.cloudshield.com/what_we_do/faq.html. (March 22, 2002).

[10] Greene, Tim. *Cloudshield device delivers faster network-based security.* 2001. URL: http://www.nwfusion.com/edge/news/2001/122589_07-09-2001.html. (March13, 2002).

[11] Network-1. *Intrusion Prevention Systems.* 2001. URL: http://www.network-1.com/products/plus-sv.html. (March 19, 2002).

[12] Info Security Magazine. *CyberwallPLUS-SV, CyberwallPLUS-WS.* 2001. URL: http://www.network-1.com/products/screv601/sc_reprint.html. (March 19, 2002).

[13] Henderson, Tom. *Fortify Windows NT and Win2000 Security.* 2000. URL: http://www.informationweek.com/791/cyberwall.htm. (March 19, 2002)

[14] Network-1. *Frequently Asked Questions.* 2001. URL: http://www.network-1.com/products/faq_firewall.html. (March 19, 2002).

[15] Psionic. *Psionic Technologies - Products.*2002. URL: http://www.psionic.com/products/index.html. (March 20, 2002).

[16] Psionic. *Psonic Port Sentry*. 2002. URL: http://www.psionic.com/products/portsentry.html. (March 20, 2002).

[17] Psionic. *Psionic HostSentry*. 2002. URL: http://www.psionic.com/products/hostsentry.html. (March 20, 2002).

[18] Psionic. *Psionic LogSentry*. 2002. URL: http://www.psionic.com/products/logsentry.html. (March 20, 2002).

[19] Okena. *Okena Stormwatch*.2002.URL: http://www.okena.com/areas/products/products_stormwatch.html. (March 20, 2002).

[20] Okena. *Okena announces Stormsystem for integrated intrusion prevention*. 2002. URL: http://www.okena.com/areas/news/news_02_01_22.html. (March 22, 2002).

[21] Okena. *OKENA Security Solutions Stop All major Attacks in 2001 from causing network damage*. 2001. URL: http://biz.yahoo.com/bw/011218/182163_1.html. (March 20, 2002).

[22] Okena. *Okena announces Stormsystem for integrated intrusion prevention*. 2002. URL: http://www.okena.com/areas/news/news_02_01_22.html. (March 22, 2002).

[23] Okena. *Okena announces Stormsystem for integrated intrusion prevention*. 2002. URL: http://www.okena.com/areas/news/news_02_01_22.html. (March 22, 2002).

[24] Murray, Conroy Andrew. *Web Server Lockdown*. 6 Feburary 2002. URL: http://www.networkmagazine.com/article/NMG20020206S0013/2. (22 April 2002).

[25] Murray, Conroy Andrew. *Web Server Lockdown*. 6 Feburary 2002. URL: http://www.networkmagazine.com/article/NMG20020206S0013/2. (22 April 2002).

[26] Symantec. *Symantec Intruder Alert 3.6*. 2002. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=11146713&EID=0. (March 13, 2002).

[27] The NSS Group. *Symantec Intruder Alert 3.5*.2002. 2002. URL: http://www.nss.co.uk/ids/symantec_intruderalert/symantec_intruder_alert.htm. (March 30, 2002).

[28] The NSS Group. *Symantec Intruder Alert Questionnaire.2002*. URL*:* http://www.nss.co.uk/ids/symantec_intruderalert/symantec_questionnaire.htm. (March 30, 2002).

[29] The NSS Group. *Symantec Intruder Alert Questionnaire.2002*. URL*:* http://www.nss.co.uk/ids/symantec_intruderalert/symantec_questionnaire.htm. (March 30, 2002).

[30] Intrusion, Inc. *Vulnerability Assessment Overview*. 2001. URL: http://www.intrusion.com/products/productcategory.asp?lngCatId=5. (March 24, 2002).

[31] Intrusion, inc. *Intrusion, Inc Launches Security analyst 5.2 Supporting HIPAA and GLB Needs for Security*. 2001. URL: http://biz.yahoo.com/bw/011211/110072_1.html. (March 24, 2002).

[32] Intrusion, Inc. *Agentless Host Vulnerability Assessment and Analysis software*. 2001. URL: http://www.intrusion.com/products/product.asp?lngProdNmId=4&lngCatId=5. (March 24, 2002).

[33] Intrusion, Inc. *System Requirements.* 2001. URL: http://www.intrusion.com/products/technicalspec.asp?lngProdNmId=4&lngCatId=5. (March 24, 2002).

[34] Nextag. URL: <http://www.nextag.com/serv/main/buyer/OutPDir.jsp?node=&otherForm=n&doSearch=y&advanced=n&search=Security+Analyst&searchnodeid=-1>. (22 April 2002).

[35] Symantec. *Symantec Enterprise Manager 5.5*. 2002. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45&PID=110682. (March 13, 2002).

[36] NSS Group. *Enterprise Security Manager 5.1*. 2002. URL: http://www.nss.co.uk/va/symantec_esm/symantec_esm.htm. (March 24, 2002).

[37] Nextag. URL: <http://www.nextag.com/Symantec_Enterprise_Security_Manager~3215614z3znz300192zz1z300000zzmainz2-htm>. (22 April 2002).

[38] Mark Abene, Gerald L. Kovacich and Steven Lutz. Intrusion *Detection provides a pound of prevention*. 1997. URL: http://www.networkcomputing.com/815/815ws1.html. (March 20, 2002).

[39] Mark Abene, Gerald L. Kovacich and Steven Lutz. Intrusion *Detection provides a pound of prevention*. 1997. URL: http://www.networkcomputing.com/815/815ws1.html. (March 20, 2002).