A Scalable, High-Availability Antivirus Solution:

A High-performance, High-availability, Antivirus and Content Security Clustering Solution

Trend Micro, Inc.
10101 N. De Anza Blvd
Second Floor
Cupertino, CA 95014 - USA

Phone: 800-228-5651 / 408-257-1500
Fax: 408-257-2003
Web: http://www.trendmicro.com

Stonesoft (Corp. HQ)
Itälahdenkatu 22 A
FIN-00210 Helsinki
Finland

Phone: +358 9 4767 11
Fax: +358 9 4767 1234
Web: http://www.stonesoft.com

Stonesoft, Inc
115 Perimeter Center Place,
South Terraces, Suite 1000
Atlanta, GA 30346 - USA

Phone: 770-668-1125
FAX: 770-668-1131

November 7, 2000

Table of Contents

Overview

Many organizations are working hard to secure themselves from the growing threats of computer viruses, Trojan horses, hacker agents, worms, and other malicious code. Yet the headlines are dominated with news of the latest computer related disaster more frequently than at any time before. This document intends to review this problem and propose several possible solutions.

The antivirus industry has been responding to these threats with ever-quicker responses to the rapid onslaught of malicious code, while corporations establish strict virus protection policies. Yet the number of related disasters continues to grow with over $12 billion in damage in the first 6 months of 2000 alone. It is proposed that the problem may reside in the lack of more comprehensive protection measures.

Placing an organization’s entire antivirus defense at the desktop level is similar to locking all of the doors in a house… while leaving windows and other entry points open. While desktop antivirus is a necessary protection against the traditional computer virus that was typically transferred by floppy disks, etc., and the primary virus security option for highly mobile laptop users, it is important to understand the limitations of this single point of defense. Virus writers have already seen this trend in protection, and have switched their strategies to leverage other entry points into the enterprise.

The International Computer Security Association (ISCA) recently published the results of it’s annual “Computer Virus Prevalence Survey 2000”, which indicates that 87% of all major virus infections are now transmitted through e-mail. And given the speed of this electronic communication, these newer computer viruses can spread much faster than the time required to update all of the desktop and laptop systems in a medium or large organization. Recognizing this change in behavior, Trend Micro developed patented technologies in the mid-1990’s to stop viruses transmitted through email and the Internet… before they could reach the desktop.

While protecting 54% of the world’s Internet gateways, Trend Micro recognized the need for a scalable high-availability antivirus security solution, and has partnered with Stonesoft to help provide it. Stonesoft, building on the tremendously successful clustering technology of its StoneBeat FullCluster software, created the StoneBeat SecurityCluster product designed to provide the benefits of clustering technology to content security solutions such as Trend Micro’s InterScan VirusWall.

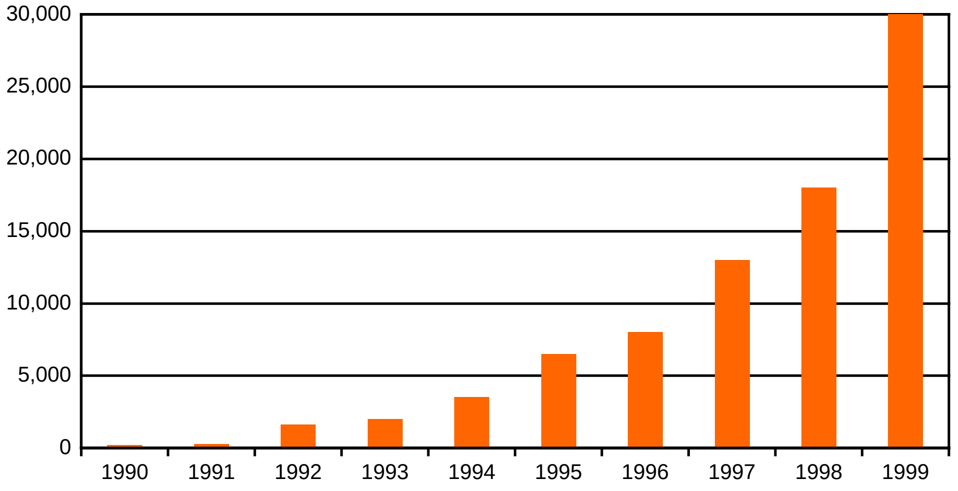
Together, the StoneBeat SecurityCluster and InterScan VirusWall provide a scalable, high-performance, high-availability clustering solution for antivirus and content scanning. These proven, award-winning technologies can meet the needs of the most demanding of environments, while their respective focus on manageability has automated many tasks and simplified administrative functions through easy-to-use interfaces developed through years of customer feedback.

The Security Threat

The "Internet Age" has arrived, bringing free flowing information to people and businesses throughout the world. And while it has unleashed new business, education, research, and communication opportunities, it has also introduced an explosion of new security threats. Many recent attacks have received worldwide attention including the Melissa virus, Love Letter, Bubble Boy, and numerous Denial of Service (DoS) attacks. Reuters reported that over $12 billion in damage was caused by computer viruses in the first 6 months of the year 2000 alone.

According to "Tippet's Law of Malicious Code", the virus problem doubles about every 14 months. Taking into consideration a number of figures from worldwide research along with its in-house numbers, Trend Micro estimates that the total number of viruses in 1999 was 30,000 (Figure 1). And research now shows that 87% of virus infections are contracted through e-mail.

Figure 1: The Growing Number of Computer Viruses



Source: Trend Micro

The intranets, extranets, and e-commerce websites that carry business-critical applications continue to proliferate. As businesses build electronic relationships with suppliers, customers and partners, the number of entrance and exit points for mission-critical information in enterprises' networks are burgeoning. The resulting complexity for IT managers attempting to implement thorough security measures, while maintain performance objectives, presents a potentially overwhelming task.

Viruses Attack Vital Resources

Computer viruses, Trojan horses and other malicious code are serious threats to worker productivity. Viruses are the most common of these threats, coming in five flavors: boot sector viruses, macro viruses, program file infectors, multipartite viruses and script viruses.

A Trojan horse is an apparently harmless program, often in the form of an e-mail message attachment, which contains malicious code. Once a Trojan gets into a computer or computer network, it can unleash a virus or other malicious code to take control of the computer infrastructure, compromise data or inflict other damage. For example, the infamous Melissa virus that struck on March 26, 1999 is a good example of a harmful Trojan. Attached to a harmless-looking e-mail message, the virus accessed Microsoft Outlook, replicated itself, and sent itself to many other users listed in the recipient's e-mail address book. The resulting e-mail flurry caused many Microsoft Exchange servers to shut down, while user mailboxes were flooded with bogus messages.

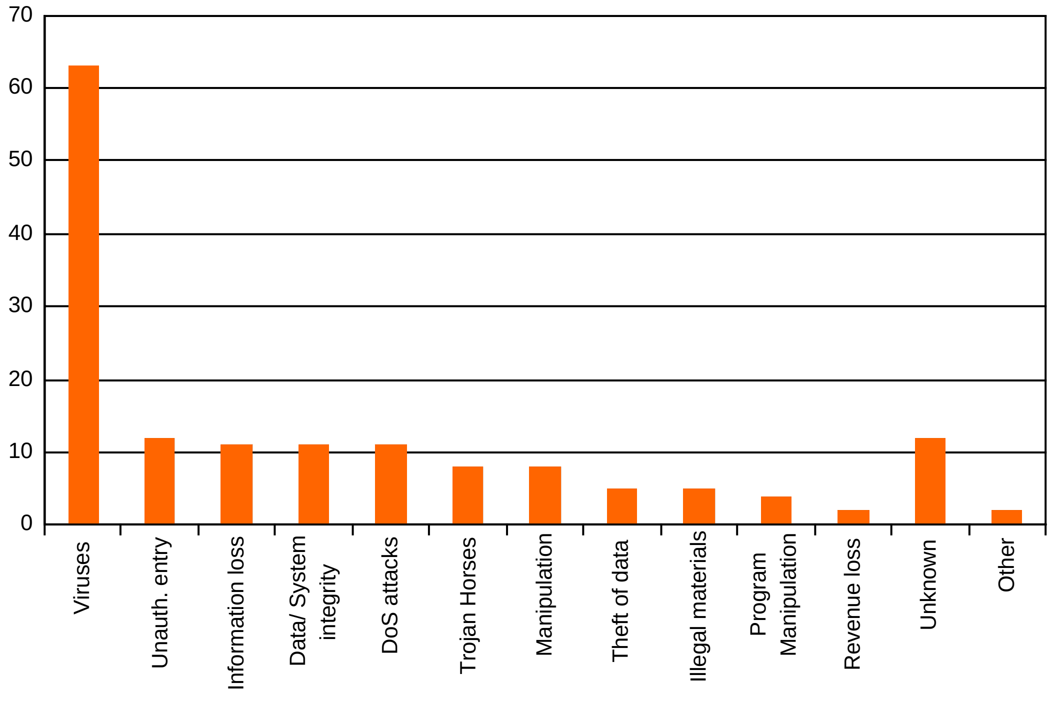
Malicious code, consisting of applets written in Java or ActiveX controls, is a new threat posed by the Internet. Code from these active content technologies often resides on Web pages and enters computer systems via the Internet to access user information. This access can facilitate legitimate business or other transactions — or can execute malicious activities such as erasing data stored on hard disks or surreptitiously copying and transmitting data to eavesdropping third parties.

If a virus infects a revenue-generating e-commerce application, resulting in downtime, the cost to the business could potentially reach millions of dollars. However, these threats not only compromise enterprise computers by rapidly infecting entire networks, they can also invite unauthorized access to sensitive enterprise information resources.

Beyond the Desktop

More desktops are protected today with antivirus software than at any other time. The vast majority of large corporations have implemented comprehensive antivirus security programs for their networked computers. Yet we have recently seen more widespread damage from major virus outbreaks than in any other time in history. Computer viruses represent the greatest security concern for IT managers today (Figure 2).

Figure 2: Business Internet Users' Security Fears



Source: Information Week Global Information Security Survey of 2700 Security Professionals, July, 1999

It is easy to see that desktop antivirus alone cannot address the overall threat. This is why IT managers are considering solutions at the gateway to block viruses “before” they can reach the desktop. They are doing this because they have identified the reasons that desktop antivirus has failed as a single, sole security measure.

Desktop antivirus solutions, when properly installed and maintained, are highly effective protection against virus threats. However, in the real world, desktop systems are constantly changing with the installation of new software, software updates, and configuration changes. These can interfere with the antivirus software's ability to detect viruses by unintentionally deactivating or blocking portions of the software that would otherwise detect a particular threat. Most often the virus pattern files -- the database that the antivirus software uses to identify what is, and is not, a virus – are out of date because the update mechanism has been interfered with. Since the antivirus software runs quietly in the background, the user is unaware when it "stops" running in the background… until they get a virus.

Part of the solution has been addressed through the development of "office" oriented solutions instead of "desktop" solutions. In addition to providing centralized management, these solutions incorporate a number of techniques that enable IT managers to verify the effectiveness of each desktop systems' antivirus installation, force updates, block user access to the antivirus software and perform other functions to insure that each desktop system is current and running correctly.

Gateway Security

The largest challenge facing IT managers regarding virus security, particularly in large networks, is the response time required to update all of the networks PCs when a new virus outbreak occurs. When a threat like the "Love Letter" virus can spread around the world in less than one hour, the time required to update all networked PCs is completely inadequate. And such an inadequacy can cost a business millions of dollars in damage.

On the other hand, a hand full of Internet and e-mail gateways can be updated in a matter of minutes. With the gateways monitoring all inbound traffic for potential threats, the desktop update process can take place to provide protection from the floppy disk or CD-ROM a user may receive tomorrow from someone with an infected system.

IT managers need to have a complete antivirus security solution, but with the numerous virus outbreaks that have occurred recently, it is clear that they must implement security systems that give them the control and the ability to respond in a major disaster situation. The gateway has become the most vulnerable point for Internet based threats.

But the gateway serves mission critical business functions. So IT managers have several key concerns about implementing such a gateway solution.

- **Stability** – Is the antivirus solution going to work smoothly with the other hardware, software, firewall and network systems?
- **Availability –** How will the antivirus solution provide scalability, maintainability, and overall availability of the core gateway function?
- **Performance –** With bandwidth at a premium, will the antivirus security solution impact the gateway's performance?
- **Scalability** – Is the solution able to grow with the company's needs? Can it do so without interrupting critical network services?

Many organizations can address these issues with minor investments in memory upgrades, configuration changes, or other common practices to support the addition of a new application on an existing system. Others may setup a dedicated antivirus system as a proxy device. But many others will need a more advanced solution to effectively support their current and long term business needs.

The Effective Security Solution

A truly effective Internet gateway antivirus security solution must be constantly active, current and in full force without causing disruptions to critical network services. A "VirusWall" must be stable and function transparently to the end user. Stability is achieved by gaining appropriate product expertise and through close attention to installation and configuration options. But transparency requires that the solution function without noticeably impacting the other network applications and services.

Today's enterprise networks must take into account the high-availability expectations for critical network services and applications. The most effective antivirus security solution will support those expectations through performance, scalability, and maintainability. Given the complexity of many of today's enterprise networks even the top performing security solutions may soon become inadequate unless it addresses these issues.

Clustering for Gateway performance and availability

There is a limit to the high-availability, scalability, and maintainability that can be achieved with a single security gateway. Even the option of upgrading hardware (with more RAM, faster processors, etc.) will require the interruption of gateway services. Therefore, using computer-clustering technology to create a "VirusWall Cluster" can offer many immediate benefits.

1. A VirusWall Cluster solution provides an enviable quality of service level through system availability by eliminating the single-point-of-failure with redundancy. Even during "scheduled shut-downs" users will continue to receive the benefits and protection of the VirusWall, while individual servers within the cluster are taken off-line for maintenance or upgrades. And during normal day-to-day operations, a VirusWall Cluster solution, utilizing Stonesoft's StoneBeat technology, provides true dynamic load balancing across the cluster to optimize the use of all available resources.

2. A VirusWall Cluster solution provides the scalability to add to the number of servers in the cluster to support increased performance demands due to company growth or simply periods of increased traffic. An unexpectedly high response to a news or industry event, advertising promotion, etc. would benefit from the temporary addition of one or more servers… rather than lose prospective business due to system "bottlenecks".

3. Clustering solutions generally offer a straightforward economic advantage by allowing the IT manager to increase performance with commodity style PCs rather than invest in larger systems that have little function beyond the original purpose for which they were purchased.

However, it is important to note that generic clustering products, while improving availability aspects, commonly create new problems for the IT manager. Therefore, it is important to choose a clustering solution designed to manage "content". The Stonesoft SecurityCluster is the only scalable high availability solution dedicated to content scanning. This paper will further discuss the characteristics of a fully engineered, proven, secure high-availability solution.

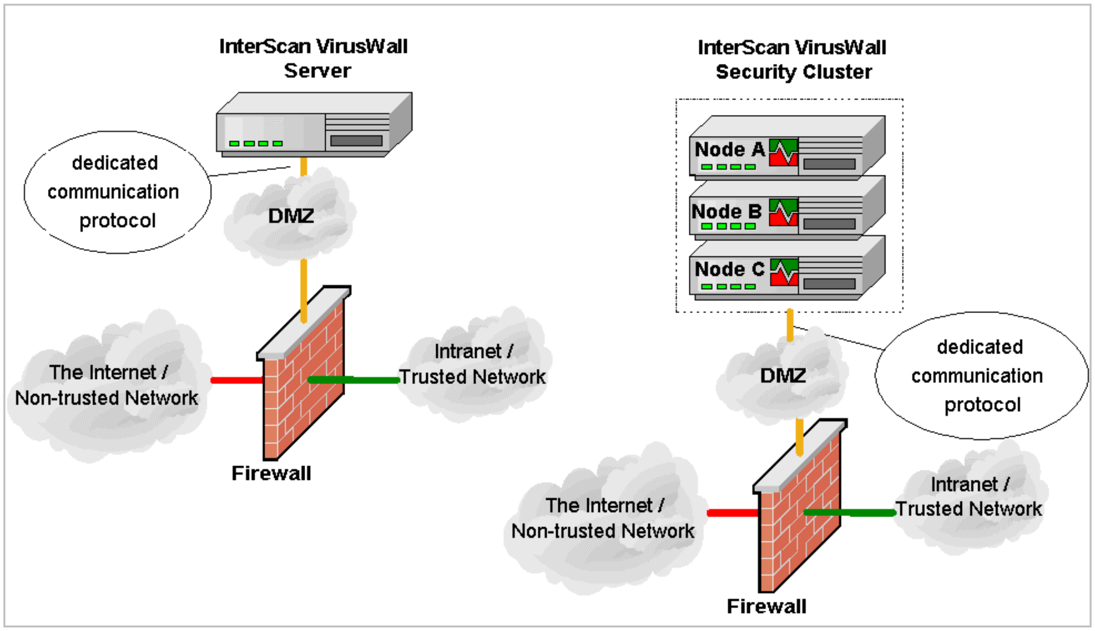
Antivirus Clustering in Practice

In general, there are three different architectural options used to set up an antivirus cluster: Vectoring Configuration, Gateway/Proxy configuration, and a Split Gateway configuration

Vectoring Configuration

A typical vectoring configuration places the antivirus solution security server in the DMZ, just behind a firewall (Figure 3). In this configuration the firewall sends any potentially harmful content or malicious code to the VirusWall for inspection before passing it on. Utilizing a dedicated communication protocol established between the firewall and the VirusWall.

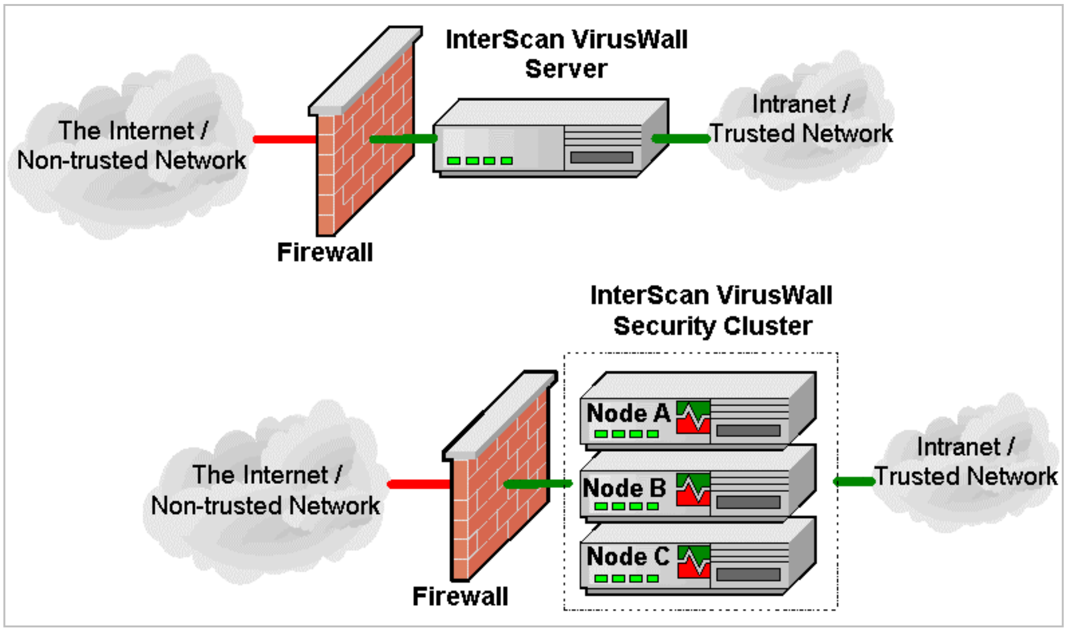
Figure 3: Security Servers in a Vectoring Configuration


InterScan VirusWall Server
dedicated communication protocol
DMZ
The Internet / Non-trusted Network
Intranet / Trusted Network
Firewall
InterScan VirusWall Security Cluster
Node A
Node B
Node C
dedicated communication protocol
DMZ
The Internet / Non-trusted Network
Intranet / Trusted Network
Firewall

Gateway / Proxy configuration

Another possible network configuration is the proxy configuration (Figure 4). In this topology the antivirus security server is on the trusted side of the network directly behind the firewall. This seemingly straightforward configuration has some evident downsides if not clustered.

Figure 4: Security Servers in a Proxy Configuration

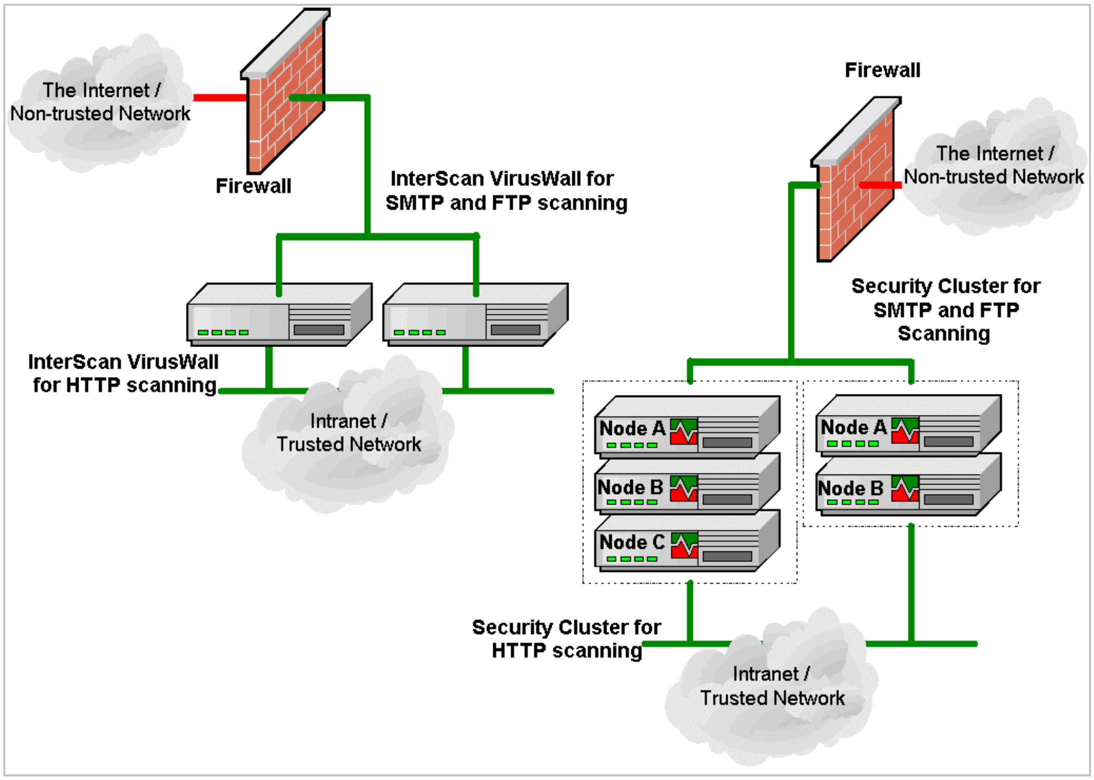

InterScan VirusWall Server
The Internet / Non-trusted Network
Firewall
Intranet / Trusted Network
InterScan VirusWall Security Cluster
Node A
Node B
Node C
The Internet / Non-trusted Network
Firewall
Intranet / Trusted Network

Recursive decompression and antivirus scanning makes antivirus protection more CPU-intensive than firewall services, which means that the security server can potentially slow down all network traffic. Further, a single security server in this configuration will take the entire network down, in the event of a security server outage (planned or unplanned). However, the StoneBeat SecurityCluster solution makes this configuration option feasible because the single point of failure is now removed and the computational performance will no longer be an issue. In fact, thanks to clustering, this configuration becomes very appealing again since it relaxes both the firewall and the virus wall from using any additional protocols for inter-communication.

Split Gateway / Task specific clusters

Quite often large corporations with intensive network traffic split the tasks and duties of gateway security servers. For example, SMTP and FTP traffic may be scanned by same the server, while HTTP traffic could be directed to another dedicated server (Figure 5). This option can improve both performance and availability to some degree. While performance is not an issue with a clustered VirusWall, clustering each security service separately offers a means to tighten the security of each system. This is important since services such as SMTP, HTTP, and FTP have different security configuration requirements. By running services on dedicated clusters, the security of those clusters can be tightened to provide only what that specific service requires.

Figure 5: Task specific security servers and clusters



The VirusWall Solution

Trend Micro's InterScan VirusWall is a server-based product that integrates information flow management with virus protection at the Internet gateway. InterScan is composed of two parts, VirusWall, which scans SMTP, FTP, and HTTP traffic for viruses and malicious applets and the optional *e*Manager – which blocks "spam", filters e-mail based on content and manages e-mail delivery.

InterScan VirusWall

InterScan VirusWall scans all relevant Internet traffic (SMTP, FTP and HTTP) for viruses and other malicious code. InterScan employs its own high speed proxy technology to catch and scan Internet traffic. By using its own proxy server, InterScan can be firewall independent. To optimize performance, InterScan VirusWall intelligently diverts only the Internet traffic capable of carrying malicious code to its scanning engine.

The heart of any antivirus product is its scanning engine. Trend Micro uses a consistent scanning engine as the core for all of its antivirus products, including the InterScan. Trend Micro's latest scanning technology is up to 50% faster than competitive antivirus scanning engines and can detect virtually all known and most unknown computer viruses. The current scanning engine supports 21 types of compressed files and reads BINHEX, UUENCODE, BASE64, and QUOTED PRINTABLE e-mail coding schemes.

Trend Micro detects new macro viruses with its MacroTrap^{TM} and SoftMice™ technologies. These tools supplements traditional pattern matching techniques with sophisticated rule-based scanning. Using MacroTrap, macro commands embedded in many word-processed and spreadsheet files are analyzed to determine whether the macro's execution would lead to malicious behavior. If so, the virus is eliminated and the file cleaned.

Virus scanning with Trend Micro products is achieved with minimal impact on network performance. In studies conducted by the National Software Testing Laboratories, InterScan has dramatically outperformed competing products in performance, detection and other key factors.

Trend Micro updates its virus pattern files on a scheduled weekly basis, with more frequent updates during virus outbreaks. Updates can be retrieved manually or automatically performed on a scheduled basis by InterScan.

Trend Micro's InterScan not only detects and blocks malicious applets, it also allows administrators to set corporate-wide policies regarding what applets will be allowed to enter the enterprise. InterScan can detect and block ActiveX applets that lack valid certificates right at the Internet gateway. It can also block unsigned Java applets. Using InterScan, administrators can even specify "trusted" domains – and block all applets from outside those domains.

InterScan *e*Manager

InterScan *e*Manager provides system administrators with the tools to block spam, prevent the release of unauthorized information and manage the delivery of large e-mails. *e*Manager consists of three modules – the spam filter, the content filter and the e-mail manager.

The Spam Filter

*e*Manager's spam filter uses both keyword scanning and lists of known "spammers" to block unsolicited bulk e-mail. Trend maintains an extensive list of known sources of spam. *e*Manager automatically retrieves updated copies of this list. *e*Manager can delete, quarantine, or archive the spam message at the Internet gateway. This eliminates the impact of unwanted e-mail on employee productivity.

The Content Filter

The content filter of *e*Manager monitors the content of outgoing e-mail. Once the administrator establishes specific keywords, identification of any keyword in any outgoing e-mail will trigger preventive action. This, too, can be tailored expressly for the corporate culture, such as quarantining the mail without delivery, deleting the e-mail, or archiving the message while permitting delivery. Customized notifications to the sender, recipient or others can also be provided. This type of diligent monitoring can effectively reduce the risk of liability due to industrial espionage, insider trading or unauthorized contacts with the press.

The eMail Manager

The e-mail manager performs both active and passive management functions. It actively performs load-balancing tasks while it passively collects and presents information that can be used for capacity planning and other management functions.

The load balancer allows the system administrator to control e-mail deliveries based on message size. The balancer can also delay delivery of e-mails with large attachments by re-configuring e-mail load balancing parameters. Managing e-mail flow will help to optimize the performance of the e-mail delivery system as well as the overall network.

The other portion of the e-mail manager gathers information about e-mail usage, such as the number or volume of e-mails sent/received by person per hour… to help identify those with heavy dependencies on e-mail as well as those who may be abusing a limited resource. All of this information, stored in an SQL database, provides the basis for the load balancing feature, allowing the IT manager or e-mail administrator to fine tune the load balancing function for maximum effectiveness, based on real experience.

Benefit Summary

Designed specifically for high-volume environments, by the only antivirus company built on server-based solutions, Trend Micro's InterScan VirusWall and InterScan eManager provide a stable security solution with minimal performance impact. Transparently blocking all viruses and malicious code, as well as providing load balancing services to optimize the e-mail and network environment, it is a solution that will definitely result in overall increased employee productivity by reducing downtime from the most common Internet threats.

Founded on a philosophy of central management and the automation of common functions, such as pattern file updates, limited IT resources can focus on other, high priority projects.

All of these benefits are further enhanced by Trend Micro's close partnering with OS manufacturers, hardware manufacturers and other industry leaders and innovators, such as the clustering technology from Stonesoft. For those organizations requiring even higher levels of high-availability, scalability, maintainability, transparency, and performance, such relationships provide IT managers with the security that the combined solutions truly work together to provide the best possible solution.

The StoneBeat Cluster for Trend Micro's InterScan

StoneBeat™ SecurityCluster ® - *The Scalable High Availability Solution for Security Servers* is a software solution that was developed for building continuously available security server systems via applicable hardware and operating systems. It is based on the same, proven, cluster technology as StoneBeat FullCluster for FireWall-1.

Since Stonesoft launched its StoneBeat high availability cluster technology in 1996, it has become a benchmark for the industry and has come to dominate the software-based high availability segment of the network security market with over 90% market share.

Requirements of a fully-engineered cluster solution

What are the design specifications for an easy-to-deploy and robust high availability solution for security gateway applications? What are the pertinent characteristics that constitute the overall quality of a cluster solution beyond high availability?

One of the basic design specifications for StoneBeat high availability architecture has been an inherently redundant topology. Common load balancing and high availability solutions based on a central dispatcher are, by their nature, introducing a minimum of one new single-point-of-failure. In order to introduce any redundancy to increase system availability, you must bring in even more new components into the network architecture. By contrast, the StoneBeat solution deploys as a fully distributed architecture, utilizing a load-balancing algorithm and placing fail over control in the form of "agents" in each and every server. This also removes the need for any new hardware to achieve operational redundancy of clustered servers.

Some additional, highly desirable, features for any clustering technology for security servers include:

1) Total transparency – As part of an effective security solution the clustering has to remain invisible to the users of the service and to all other network components.
2) Easy Administration –A clustering solution should simplify network administration rather than increase the management workload or add to the complexity of the network architecture. This applies to both "time" and the demands placed on network "resources" to handle the management tasks.
3) Extensive Failure Detection – Failure detection capability should go beyond application specific failures or common hardware failures (such as disk failures). It should also be able to recognize NIC failures, downstream device problems, and identify path access failures.

Solution that works

The StoneBeat SecurityCluster has a single layer 2 MAC address and, respectively, a single layer 3 IP address. This means that the entire cluster is seen, regardless of the number of nodes, as a powerful single-ID machine that is always up and available. The load-balancing agent (filter) resides on each node (server) of the cluster right next to network adapters and before the TCP stack.

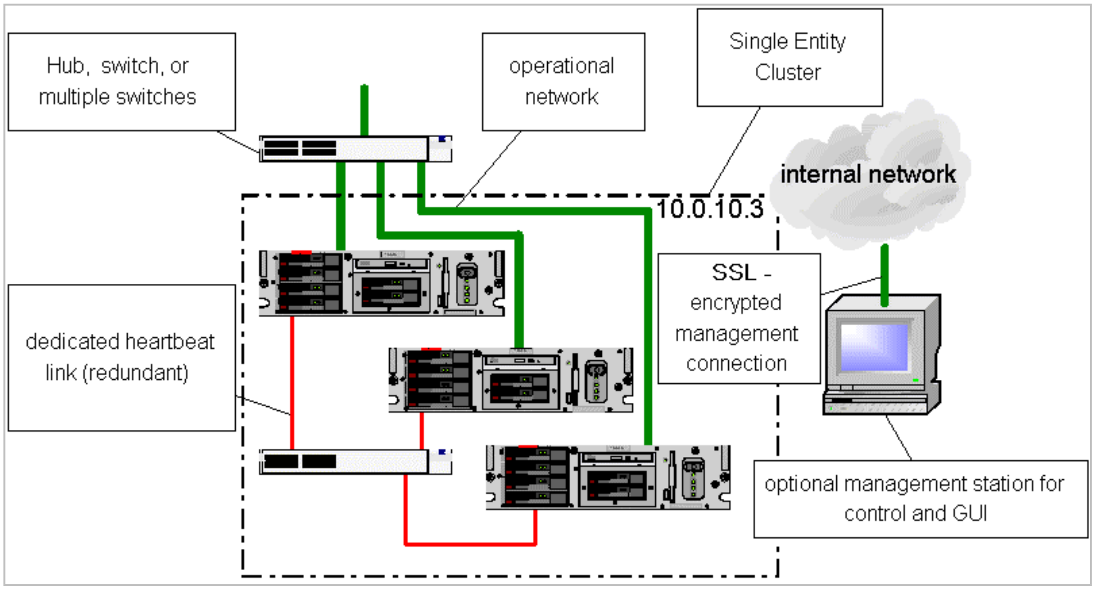
The incoming traffic is delivered to all nodes by using a multicast subnet. Only one server will process a packet while the load-balancing filter tells the other nodes to simply ignore it. This methodology maximizes throughput by filtering unwanted packets faster than it would take to manage the routing of packets to individual nodes. It is easy to see that this architecture also helps resolve the first two design criteria discussed earlier… total transparency and reduced management overhead.

Total Transparency:

Scaling up from a single content security server to a cluster solution, whether as a standalone gateway or in conjunction with firewalls, will occur without being noticed by users or impacting the functions of other network components. No changes are required to other network components since the cluster can assume the existing IP/MAC addresses. Any configuration changes to the cluster, such as adding new nodes to a server or taking a node off-line for servicing, are completely invisible to other network components or users. In the same fashion, a node fail-over within the cluster has no impact (e.g., packet re-addressing) upstream or downstream of the content security servers.

Finally, an optimal utilization of available resources requires true dynamic load balancing, which means a continuous, even distribution of active connections. All load redistribution within a cluster occurs unnoticeably. With a totally transparent cluster technology, like StoneBeat, it makes no difference to other network components as to which node serves a particular connection.

Figure 6: Security Cluster Environment


Hub, switch, or multiple switches
operational network
Single Entity Cluster
internal network
10.0.10.3
SSL - encrypted management connection
dedicated heartbeat link (redundant)
optional management station for control and GUI

Easy Administration

Software or hardware maintenance with rolling upgrades during normal business hours is a routine task. While maintaining transparency, a node or segment of a cluster can be set to offline, the upgrade performed, tests executed, and then it is brought back on-line by an administrator.

The StoneBeat SecurityCluster takes this process one step further with the ability to turn off a node from an easy-to-use Java GUI or using a command line. Graceful shutdown ensures that all existing connection transactions are completed and new ones moved to the other nodes before the node that is being serviced goes off-line. More commonly used “brute force” methods would simply drop all the connections.

Configuration changes (e.g., adding new nodes) do not require the reconfiguration of routers as required by many IP pooling technologies. And, because the load balancing functionality is distributed and integrated into each security server, the StoneBeat SecurityCluster does not add to the complexity of the network architecture as a “central dispatcher” clustering approach does.

Extensive Failure Detection

Successful resource management must rely on a feedback system. This makes resource monitoring one of the most important aspects of proper clustering. The capability of detecting software failures (e.g., temporary failures due to overload conditions) or hardware failures (such as NICs or downstream devices) is essential. This is why StoneBeat clustering deploys resource resident monitoring to provide availability monitoring within each node. External monitoring is a commonly used, but less effective technique, since it is limited to evaluate responses to inputs to each cluster node.

The extensive StoneBeat test subsystems go beyond network interfaces and application software-testing key components of the operating system, such as CPU utilization and file systems. Administrators can configure custom tests by integrating executable programs or scripts. And all of these tests can be grouped with logical operators to create even more exhaustive test and decision conditions.

Benefits summary

StoneBeat SecurityCluster ensures that InterScan VirusWall antivirus protection is always on-line. The potential vulnerability of system availability with a server-based antivirus solution is relaxed with system redundancy. This allows taking full advantage of centralized antivirus protection at the Internet gateway with InterScan VirusWall and no downtime issues.

StoneBeat SecurityCluster ensures that the InterScan VirusWall antivirus protection is never the network traffic bottleneck. The dynamic load balancing distributes the content scanning evenly across a VirusWall security cluster while taking into account the relative capacity, system utilization and available memory at any given moment with each node. This means maximized throughput with available resources. The gateway performance can be further enhanced with a proxy configuration of the security cluster; no overhead of a dedicated communication protocol neither with the firewall or the InterScan VirusWall.

InterScan VirusWall and StoneBeat SecurityCluster provide a scalable enterprise antivirus security solution. New nodes and more computational power can be added to VirusWall SecurityCluster as needed. No changes to other parts of network are necessary, meaning tremendous flexibility to adjust to future network configurations and virus protection needs.

StoneBeat SecurityCluster secures the InterScan VirusWall investment for the future. The existing system can be expanded with no need to replace or upgrade the existing nodes. The bundling of last year’s “biggest and baddest” hardware at devaluated prices gives a performance/cost advantage over today’s top performers. The coverage of StoneBeat clustering technology ranges from firewalls and security servers, to Web, cache, and database servers clustering with a single GUI management. This ensures that the security cluster can be a part of an enterprise strategy, not a one-time solution.

InterScan VirusWall gateway protection, fortified with StoneBeat SecurityCluster will ease the network administrator from unnecessary burdens, with centralized administration, automation of routine tasks, and in inherently redundant, high-availability architecture. By viewing the “big picture” of the content security and the system availability problem, it is easy to see that resolving the problem at the system level makes for a much more simple solution. Fully engineered solutions for complex environments simplify the problem domain.

Additional References

Aberdeen Group, “Trend Micro: The Prescription for the Virus Plague,” 1999, (http://www.aberdeen.com)

Computer Economics, “Malicious Virus Attacks Cost Organizations More Than $12 Billion in 1999,” January 14, 2000, (http://www.computereconomics.com/new4/pr/2000/pr000114.html)

Messaging Online, "Messaging Today," Volume 2, No. 20, November 29, 1999, (http://www.messagingonline.com/mt/html/mt112999.html)

National Computer Security Association, "Third Annual ICSA Computer Virus Prevalence Survey: 1997," 1997, (http://www.isca.net)

International Computer Security Association, "Fifth Annual ICSA Computer Virus Prevalence Survey: 1999," 1999, (http://www.isca.net)

ZDNN, “Web attacks: Are ISPs doing enough?”, February 21, 2000, (http://www.zdnet.com/filters/printerfriendly/0,6061,2444159-2,00.htm)

About Trend Micro, Inc.

Trend Micro Inc. provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, e-mail servers and file servers, Trend Micro allows companies worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop.

Trend Micro has extensive after-sales technical support via our website, e-mail and telephone. Customers are entitled to free virus pattern and program updates for a period of one year, and can access a database of previous technical support questions via their web browser. Newsletters that contain the latest virus information are available on the web or via e-mail and electronic product documentation files can be downloaded for free. For more information about technical support available to Trend Micro’s customers, visit http://www.antivirus.com/support.

Trend Micro’s award-winning products have been chosen by Check Point, Hewlett-Packard, IBM, ISS, Lotus Softswitch, Microsoft, Netscape, Oracle, Sun Microsystems, Wingra and WorldTalk as a key part of their server security solutions. Trend Micro is publicly traded on the Tokyo stock exchange and has offices worldwide. North American headquarters are in Cupertino, Calif.

Many Trend Micro products — including InterScan VirusWall — can be test-driven online in Trend Micro’s Virtual Lab at http://virtual-lab.antivirus.com. Additional information about Trend’s products can be obtained at http://www.trendmicro.com, by sending e-mail directly to info@trendmicro.com or by calling 1-800-228-5651 or (408) 257-1500.

About Stonesoft Corporation

Stonesoft Corporation (HEX: SFT1V) is a global Finnish software company headquartered in Helsinki, Finland and Atlanta, Georgia. Stonesoft is the leading innovator and provider of software-based, high availability network security and e-business solutions for telecommunication companies, financial institutions, high volume Internet sites and large enterprises deploying Internet-based applications. Stonesoft's StoneBeat product line is the worldwide technology and market leader, being the only software product that combines dynamic load balancing and high availability for firewalls and other applications, such as web, cache, content scanning and DNS servers.

Stonesoft markets its own products - StoneBeat and Optiwise - on a global basis and is a Nordic distributor for the solutions of world market leaders. Stonesoft has European offices in the United Kingdom, Germany, France, Spain, Italy, Sweden and Norway; and in the Far East/Pacific Rim in Singapore, Japan and Australia. Its research and development centers are located in Helsinki, Finland; Sophia Antipolis, France; and Florence, Italy.

For more information about Stonesoft Corporation and its products, please visit http://www.stonesoft.com or http://www.stonebeat.com.