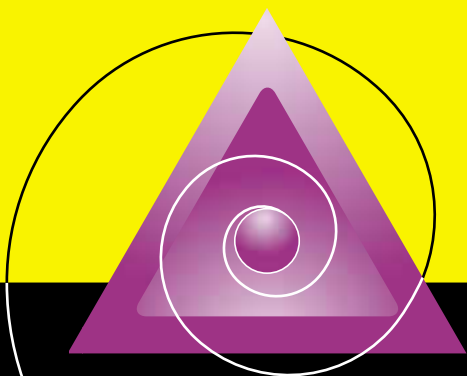


Visit techguide.com

The
Technology
Guide
Series

 a product of
newmediary®

Stopping Attacks: The Importance of Denial of Service (DoS) Security Appliances



This Guide has been sponsored by

**Top
Layer™**

perfecting the art of network security



THE ATTACK MITIGATOR FROM TOP LAYER
STOPS DoS ATTACKS COLD

Introducing the Attack Mitigator™ from Top Layer. For more information, call 1-888-327-9638, or visit us at www.TopLayer.com

**Top
Layer™**

perfecting the art of network security

Visit our Web site
to read, download,
and print all the
Technology Guides
in this series.



techguide.com

Over 100 Technology Guides in the
Following Categories:

- Software Applications
- Network Management
- Enterprise Solutions
- Network Technology
- Telecommunications
- Convergence/CTI
- Internet
- Security

● Table of Contents

Abstract	4
Introduction	5
A Closer Look at Denial of Service	9
Business Issues at Stake	10
Legal Ramifications of Compromised Security	15
Optimizing Security	17
Summary	18
Glossary	20

Editorial Writing Team

Newmediary's Technology Guides and White Papers are produced according to a structured methodology and proven process. Our editorial writing team has years of experience in IT and communications technologies, and is highly conversant in today's emerging technologies.

The Guide format and main text of this Guide are the property of Newmediary, Inc. and is made available upon these terms and conditions. Newmediary, Inc. reserves all rights herein. Reproduction in whole or in part of the main text is only permitted with the written consent of Newmediary, Inc. The main text shall be treated at all times as a proprietary document for internal use only. The main text may not be duplicated in any way, except in the form of brief excerpts or quotations for the purpose of review. In addition, the information contained herein may not be duplicated in other books, databases or any other medium. Making copies of this Guide, or any portion for any purpose other than your own, is a violation of United States Copyright Laws. The information contained in this Guide is believed to be reliable but cannot be guaranteed to be complete or correct. Any case studies or glossaries contained in this Guide or any Guide are excluded from this copyright.

Copyright © 2002 by Newmediary, Inc.
313 Washington Street, Suite 260, Newton, MA 02458
Tel: (617) 395-7900, Fax: (617) 928-5080
E-mail: info@techguide.com, Web site: <http://www.techguide.com>

Abstract

The migration from private to public networks has created new security and performance challenges for large enterprises, service providers and carriers. Recent high-profile security breaches experienced by prominent companies dependent on Internet commerce reveal the inherent vulnerabilities of operating business-critical applications over public IP-based networks. Existing firewall technologies are critical as a first line of defense for any business but are not enough to completely secure the enterprise against ever-increasing external threat of DoS attacks while maintaining high application availability and performance.

Meanwhile, the ever-growing number and types of DoS and Distributed Denial of Service (DDoS) attacks continue to bring down worldwide networks at an alarming rate. Within the last year, nearly 40 percent of all businesses with an Internet presence experienced at least one DoS attack, with a total cost in terms of lost business and shaken customer confidence in hundreds of millions of dollars. While many of these companies had taken the first steps toward securing their networks with firewalls, this technology alone was not enough to protect them against concerted and frequent DoS attacks to their networks.

Leading firewalls provide protection against a limited DoS attack. Nevertheless, they can be overwhelmed by a major attack mounted from multiple Internet-based systems. Furthermore, the processing power consumed by the firewall in trying to protect against a major DoS attack – something no firewall was designed to do inherently – can bring the network to a crawl. The solution is to augment a firewall with security appliances optimized to recognize and thwart a broad array of server-targeted attacks. Such a system can potentially reside between the firewall

and a company's routers to watch for the signatures of a DoS attack by using a combination of packet filters, packet sequence signatures, HTTP URI filters, TCP connection counters and threat-level assessment based on network connection behavior. Once malicious traffic is identified by a security appliance, it is discarded, allowing legitimate traffic to proceed through the network and devices at Gigabit speeds.

This Technology Guide begins by outlining the history and extent of the DoS problem. Next, it examines how a network can be secured against all types of DoS attacks by employing firewall and DoS mitigation systems together. It presents how the solution meets the varying application performance and security needs of enterprise customers, service providers and carriers. Finally, this Guide illustrates the business benefits of deploying DoS mitigation security appliances as opposed to using firewalls alone.

Introduction

The rapid growth of the Internet has fuelled the demand for universal connectivity. However, the open environment of the Internet is a double-edged sword. While the migration from private to public networks has made it possible for any organization to extend the global reach of its business, it also exposes the enterprise to a larger variety of security threats. The recent number of high-profile security breaches experienced by prominent industry players reveals the inherent vulnerabilities in operating business-critical applications over public IP-based networks. According to a study conducted by the Computer Security Institute, 90 percent of the 650 companies surveyed had detected computer security breaches during the previous 12 months. The same study found that 74 percent acknowledged financial

losses due to these security breaches. Although only 42 percent were able to quantify their losses, the financial losses reported by 273 respondents totalled more than \$265 million. This is the proverbial tip of the iceberg.

Many organizations think that if they have a firewall or intrusion detection system (IDS) in place, then they have covered their security bases. Experience bears out that this is not the case. While important, a firewall alone cannot provide 100 percent protection. In addition, the rate at which new security threats are unleashed into the public Internet is phenomenal. Yesterday's security architectures and general purpose tools cannot keep up. For this reason, incumbent network security policies and systems require ongoing scrutiny in order to remain effective. As Internet access continues to expand and the quantity and speed of data transfer increases, new security measures must be adapted. In order to understand how best to secure the enterprise against newer-generation security threats, it is first necessary to understand the nature of the problem.

The Nature of the Problem

By embracing the Internet, large enterprises along with service providers and carriers continue to experience new business opportunities and growth. The enterprise network and the applications that run over it have become business critical, an essential part of an organization's strategy to increase revenues and, ultimately, profits. Not only can a company reach a larger number of customers via the Internet, it can serve them faster and more efficiently. At the same time, using a public IP network enables companies to reduce infrastructure-related costs.

Unfortunately, the same advantages that the Internet brings to business also benefit the hacker groups who propagate their attack techniques via the same public infrastructure. Hacker attack tools

are readily available on the Internet, including the development source code. Work on these GUI-based tools is often split across groups of novice hackers — known as “script kiddies” or “larval hackers” — who are scattered across the globe, providing around-the-clock progression of automated attack methods. In addition, many of the newer hacking methods utilize the distributed nature of the Internet to launch DoS attacks against unprotected organizations.

Security Threats Defined

The threats to an organization's networks are varied and numerous:

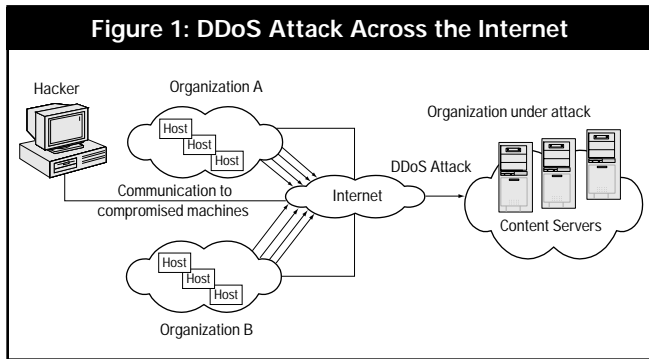
Denial of Service

One of the more prevalent methods currently used by hackers, the DoS attack floods the network and ties up mission-critical resources used to run Web sites or enterprise applications. In some cases, vulnerabilities in the Unix and Windows operating systems are exploited to intentionally crash the system, while in other cases large amounts of apparently valid traffic are directed at sites until they become overloaded and crash. Forms of DoS attacks include: Ping Flood or Ping of Death, SYN Flood, UDP Flood and Smurf Attack.

Distributed Denial of Service

Another form of DoS is the DDoS attack. This uses an array of systems connected to the Internet to stage a flood attack against a single site. Once hackers have gained access to vulnerable Internet systems, software is installed on the compromised machines that can be activated remotely to launch the attack. Although recent DDoS attacks have been launched from both private corporate and public institutional systems, hackers tend to favor university networks as launch sites because of their open, distributed nature. Programs used to

launch DDoS attacks include Trin00, TribeFlood Network (TFN), TFN2K and Stacheldraht.



Network Intrusion

To launch DDoS attacks, hackers first gain access to the systems unwillingly drafted for these malicious purposes. Network intrusion methods come in many forms:

- **Network scanners and sniffers:** These tools can be used by hackers to discover vulnerabilities that may exist in network hardware and software configurations.
- **Password cracking and guessing tools:** Password crackers such as L0phtcrack and John the Ripper use dictionary cracking and brute-force cracking methods to discover network passwords.
- **IP spoofing:** This technique is used to gain unauthorized access to computers, whereby the intruder sends messages to the target computer after forging the IP address of a trusted host by modifying the packet headers so it appears that the packets are coming from that port. IP spoofing is a key tool used by hackers to launch DoS attacks.

- **Trojan horses and malicious Java/ActiveX applets or Visual Basic scripts:** These weapons can pose as benign applications, often attached to e-mail messages, and be launched remotely by a hacker for destructive purposes.

Viruses and Worms

Other vexatious forms of security threats include viruses and worms — malicious programs or pieces of code usually propagated via e-mail or HTTP packets. After being loaded onto an unsuspecting recipient's computer, a virus can often replicate itself and manipulate the computer's e-mail system to disseminate the virus to other users. Some viruses are capable of transmitting themselves across networks and bypassing security systems. Although data corruption tends to be the end goal of most viruses, a simple virus that reproduces itself over and over can be dangerous because it will quickly use all available system memory and will crash the computer. A worm is a special type of virus that can replicate itself and use up memory, but cannot attach itself to other programs.

● A Closer Look at Denial of Service

No matter which tools a hacker group may employ to launch a DoS attack on an organization, the means to achieve the desired result — a devastating traffic flood to the network — are the same. They include a single packet, a sequence of packets or a particular application connection behavior. The hacker's objective in all cases is to overload resources on a given server or network by quickly filling up the state tables. Unlike legitimate Internet traffic, which relies on a series of handshakes among the server and connected

devices to achieve communications, a DoS attack foregoes many of these handshakes by flooding open sockets that are trying to establish legitimate connections. When such an attack is at its peak, the disturbing result is that little or no real customers can connect to the network.

Because of the potentially heavy damage that DoS attacks can produce, some protection has been added to leading firewalls as well as to the server operating systems themselves. With Windows NT Service Pack 4, for example, Microsoft introduced some built-in protection for WinNuke Attack, a form of DoS attack. However, simply protecting the OS does not automatically afford the same level of protection to certain routers, cable devices, printer queues or other devices that may be attached to a company's network. The longer these devices have been in service, the greater the damage potential is even from older attack strategies.

Business Issues at Stake

Given the mission-critical nature of today's business networks, security threats that either cripple systems or violate data safety and integrity are among the biggest issues facing large enterprises, service providers and carriers today.

Most organizations have recognized the need for firewalls and IDSeS to secure their networks. However, what many companies fail to recognize is that isolated solutions do not in themselves provide absolute security against DoS attacks. They address only specific parts of the entire security problem and therefore require complementary technology to guard against attackers intent on harming a business.

Firewalls

Firewalls, are designed primarily to prevent unauthorized access to private networks by analyzing packets entering the network and blocking those that do not meet predefined security criteria. For this reason, no business on the Internet today should be without firewall protection. One of the key roles of a firewall is to specifically prevent unauthorized Internet users from accessing private networks, especially intranets, via Internet connections. Firewalls are generally considered to be the first line of defense in protecting private networks.

Intrusion Detection Systems

IDS solutions detect suspicious activity in real-time by cross-analyzing network activity against a database of traffic profiles associated with different attack methods and patterns of "normal" activity. Intrusion detection is generally installed in series with firewalls, helping to measure the effectiveness of the security system and to identify necessary enhancements.

Access Control

Apart from firewalls, other network access control mechanisms include user authentication and authorization systems used in conjunction with remote access servers.

Antivirus

Antivirus solutions scan incoming traffic, such as e-mail, for viruses, worms and other malicious file attachments. These typically come in the forms of Trojan horses, Visual Basic scripts, and Java or ActiveX applets.

Encryption

Cryptographic solutions encrypt sensitive private information while it is being transmitted over private and public networks. Forms of cryptography include public-private key encryption and digital certification.

Limitations of Existing Security Solutions

Apart from providing only part of the overall security system needed to secure today's business networks, most security methods in use today are limited in terms of functionality, capacity and performance.

For example, most firewalls use packet-filtering techniques to accept or deny incoming packets based on information contained in the packets' TCP and IP headers, such as source address, destination address, application, protocol, source port number or destination port number. Firewalls and IDS solutions take this to the next level with intelligence capabilities that allow them to look more deeply into packets and provide more granular application traffic analysis. However, this often causes network latency problems for these solutions alone.

In order to determine if a flow is legitimate traffic, an intelligent firewall needs to analyze a series of incoming packets in sequence before allowing or blocking each packet's entry into the network. This can take its toll on the firewall's server processor. If a firewall has to wait for five or six packets to line up before making the appropriate determination for each packet, this creates a 500 to 600 percent increase in network latency. This traffic flow slowdown is counterproductive to the increased bandwidth provided by today's high-speed WAN environments. At speeds approaching a full T3 line (45Mbps), today's firewalls do not have the throughput to keep pace, especially when network traffic consists primarily of small packets. With LAN speeds and Internet link speeds pushed to 100Mbps and beyond, security filtering platforms need to be accelerated to keep up with the flow.

An additional limitation in most existing IDS solutions is the inability to entrap network intruder data and redirect it to a secure location in order to perform forensic analysis. This can be key to

discovering network intrusion patterns and guarding against future attacks. Furthermore, a current trend by organizations to centralize antivirus protection on server or firewall systems further contributes to overall network latency due to system bottlenecks.

Reinforcing the Infrastructure with Appliances

To guard against the types of latency problems experienced by firewalls, any complementary security solution needs to detect all forms of DoS attacks on a high-performance hardware platform. This concept, introduced earlier, is referred to as a DoS security appliance. By offloading packet filtering and forwarding to specially-designed appliances, DoS attacks can be stopped and firewalls, routers and other devices can be freed to do what they do best. Switching data flows based on traffic type requires very high-speed processing and swift analysis of traffic by an intelligent switching engine. A hardware-based security solution that uses custom-built application specific integrated circuits (ASICs) potentially can support Gigabit-speed intelligent processing of network traffic. Furthermore, these security appliances should be easily configured to reflect the changing needs of a network's evolving security policies. By defining a central policy of offloading DoS detection and mitigation to high-powered security appliances, the throughput problems of today's firewalls and IDS systems are minimized.

The attack mechanisms employed by any DoS attack can be readily identified by such a platform. Today's security appliances must be quick and easy to configure to recognize attacks by using a built-in library of packet filters, packet sequence signatures, HTTP URI filters, TCP connection counters and threat-level assessment based on TCP connection behavior. Once the traffic is identified, it can be discarded or redirected to a safe zone for

off-line analysis by network operators, thereby allowing legitimate traffic to proceed unimpeded through the network.

Because most organizations have already invested heavily in their existing firewall and network device architectures, the introduction of a new hardware device designed specifically for DoS attack recognition and mitigation needs to fit seamlessly into this existing environment in order to be effective. Examples include:

- No changes to the existing routing infrastructure should be required.
- Appliance event logging should be integrated with the company's existing firewall logging system.
- Ease of installation by existing IT operations staff should be possible, with procedures prompted by software wizards and an intuitive, browser-based GUI.

recognize authorized remote users as they log onto the network and to have their application-specific access and usage privileges in place.

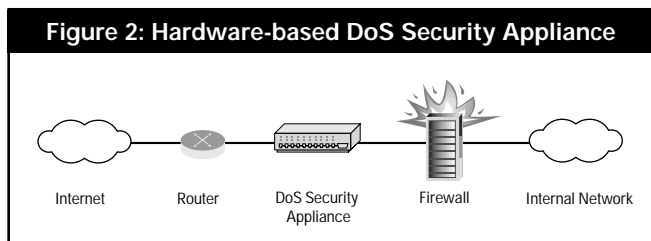
Additional functionality theoretically made possible by this new security solution is the ability to not only detect and deflect DoS attacks but to stop propagation of networked-based worms as well. The device can include a URI character string match to hunt down patterns unique to worms such as Code Red and Nimba. In this way, the device can be set up to detect specific signatures within an HTTP packet and prevent worms from connecting to Web servers. Furthermore, DoS security appliances must be extensible by network personnel via simplified configuration procedures and in-field software upgrades to recognize future worm-based patterns as they are released on the Internet.

Legal Ramifications of Compromised Security

Many IT managers still need to be educated about the potential risks to their networks, particularly the risks associated with DoS and DDoS attacks that firewalls cannot guard against alone. This may be an uphill battle. According to a recent survey by RHI Consulting, 91 percent of 1,400 CIOs polled said they are confident their companies' networks are secure. Research by the SANS Institute shows that senior executives often make dangerous assumptions that lead to computer security vulnerabilities. Common missteps include:

- Relying primarily on a firewall
- Pretending a security problem will go away if ignored

Figure 2: Hardware-based DoS Security Appliance



This new security architecture is now able to examine growing traffic volumes quickly and in fine detail. In this way, inspection priorities can be set by application type, so that, for example, TCP traffic is handled as a higher priority than UDP traffic. In the same manner, a company can choose to give higher priority to SMTP e-mail traffic over general HTTP traffic if it makes business sense to do so. Furthermore, the new security solution needs the intelligence to

- Authorizing reactive, short-term fixes so problems re-emerge rapidly
- Failing to deal with the operational aspects of security, by making a few fixes and then not allowing the follow-through necessary to ensure the problems stay fixed
- Failing to recognize the true value of their information and organizational reputation

While placing a dollar value on a tarnished corporate reputation is difficult, it is easier to understand the costs associated with lost or corrupted data. The types of assets that can vanish through electronic crime include:

- Banking and financial transaction data
- Information related to a company's competitive position
- Intellectual (processes, methods, trade secrets, proprietary data, and other intangible assets)
- Litigation-sensitive documents
- Personal identification data (whose loss can lead to "identity theft" or stalking)
- Command and control system data for satellite-systems and aircraft

The potential unauthorized release of litigation-sensitive documents in this list is only one small example of how a company can be legally compromised. Executives and organizations that are negligent in protecting corporate assets or private information from intrusion or illicit distribution face a large legal exposure. There is a fiduciary responsibility that officers of a company have to protect customer, employee, trade and other information. If negligence is proven, a breach in this trust could be catastrophic. Were the victim to sue for damages, a jury could feel justified in rewarding both compensatory and punitive

damages. As many corporate litigation cases have proven, this exposure is often in the millions of dollars. Even when an organization or corporate officer wins at trial, the legal fees generated in the process can easily reach seven figures.

Also to be considered are the costs incurred by network outages brought on by DoS attacks and related security violations. According to a Disaster Impact Research Report released by Contingency Planning Research, the business costs of network outages can be huge. In the case of credit card sales authorization systems, the average business cost for one hour of downtime can be \$2.6 million. Brokerage operations can lose \$6.45 million in business during a one-hour outage. The average hourly cost impact for telephone ticket sales systems and airline reservation centers is \$69,000 and \$89,500, respectively. Beyond quantifiable revenue losses, there are many intangible costs associated with network downtime and data theft. In addition to a blemished reputation, organizations may suffer from lost employee productivity, lost future business, potential liability due to mismanagement of client resources, and possible lawsuits and regulatory actions.

● Optimizing Security

Security preparedness has become a mandatory operational criterion for businesses that are increasingly dependent on the security and reliability of their computer networks. Properly implemented and managed, a best-of-breed security solution offers innumerable benefits both by deterring attacks and diminishing the effects of an intrusion, should one occur. Apart from guarding against the cost impact of network intrusions, a well-managed firewall environment properly reinforced with one or more dedicated DoS mitigation appliances offers the best overall

security system available today. Such a system is able to recognize and defeat most known DoS attack mechanisms and is adaptable for future attack types.

From a human resources perspective, staffing and training costs are minimized because the additional appliances that protect against DoS attacks fit seamlessly within the existing network infrastructure, thereby requiring no additional technical hires. By employing browser-based management software, the devices can be managed by the existing operations staff who can view traffic and attack status graphs to quickly pinpoint what kind of attack may be happening.

Besides the quantifiable cost savings made possible by reducing or eliminating the threat of DoS attacks are the more intangible benefits of generating goodwill. Customers will be eager to do business with an organization providing secure and fast access to network resources. By reducing revenue losses due to network outages and guaranteeing a high standard of service quality, companies can continue to grow their Internet business with confidence.

Summary

Many companies reaping the benefits of Internet commerce do not understand the true costs that are associated with the growing number of DoS and DDOS attacks that continue to bring down Internet sites worldwide. Even a few minutes of downtime can be expensive when millions of dollars of business transactions is shut down as a result of a hacker attack. Just one attack that takes longer to detect and rectify can be even more disastrous — not just in terms of lost revenue but in terms of intangibles such as loss of customer confidence, the distinct possibility of unfavorable media coverage, potential legal liability and

reduction in employee productivity. When a company loses its entire customer support operation for even one hour, the costs can be astronomical both in immediate lost revenues and damage to brands that may take years to build back up.

Yet the danger continues. Within the last year, nearly 40 percent of all businesses on the Web experienced at least one DoS attack, with a total cost in hundreds of millions of dollars. Existing firewalls were not designed to secure the organization against DoS and related attacks however, many executive managers still believe that firewalls adequately protect against DoS attacks, without understanding the potential negative impact on network availability, cost of security attacks or the degradation of their security investment.

Fortunately, the risks can be minimized by combining firewalls with DoS security appliances built from the ground up to guard against DoS intrusions. In this way, an organization can increase its network security considerably with little or no changes to its overall network infrastructure. By combining firewalls with high-speed hardware-based DoS security appliances, new levels of protection can be achieved at unmatched speeds over Gigabit links. Companies that harden their networks in this way are more impervious to hacker and other forms of malicious traffic, much better protected against downtime and more likely to be insulated from costly and embarrassing legal liabilities. At the same time, the added protection fully leverages existing firewalls without need for additional software expenditures, and the existing network operations staff can be utilized with minimal need for additional training. In short, by integrating such appliances with existing servers, routers and intrusion detection devices, a more secure network based on existing solutions is within reach of any organization today.

Antivirus — Software that scans incoming network traffic for viruses, worms or other malicious traffic such as Trojan horses.

Application Specific Integrated Circuit (ASIC) — A custom-built, high speed computer chip designed for a specific application.

Authentication — Verification of the identity of specific end users or systems communicating with the network.

Authorization — The granting of specific network usage privileges to end users or systems communicating with the network.

Denial of Service (DoS) — A form of network attack that floods the network with large amounts of data packets and ties up mission-critical resources, often resulting in the network becoming overloaded and crashing.

Distributed Denial of Service (DDoS) — A form of DoS attack that uses an array of systems connected to the Internet to stage a flood attack employing illegitimate network traffic against a single site.

Encryption — The use of algorithms to scramble and unscramble information to enable secure data transmission over private and/or public networks.

Firewall — Typically a software system designed to prevent unauthorized access to or from a private network. The firewall examines packets entering and leaving the network and blocks those that do not meet predefined security criteria.

Firewall Balancing — The load balancing of application traffic among multiple firewalls to increase the capacity and performance of the overall security system.

Intrusion Detection System (IDS) — A security solution designed to detect suspicious network activity by cross-analyzing inbound and outbound traffic against a database of network attack profiles.

Network Forensics — The ability to discover network intrusion patterns by analyzing intruder data entrapped in a secure network location, such as a decoy server.

Network Intrusion — Unauthorized access to private networks or computer systems, usually with the intention of stealing or corrupting data.

Remote Access — The ability to log onto a network from a remote location, often using dial-up, broadband or DSL connections.

Security Appliance — A high performance hardware platform dedicated to specific security tasks such as DoS attack mitigation. Such systems utilize leading technologies such as custom ASICs, highly optimized packet inspection software and intuitive GUI-based configuration tools.

Trojan Horse — A malicious program that masquerades as a benign application and can be launched remotely by a hacker for destructive purposes.

Virus — A malicious program or piece of code loaded onto an unsuspecting recipient's computer. Viruses can replicate themselves and manipulate computer e-mail systems to disseminate the virus to other users.

Worm — A special type of virus that can replicate itself and attack computer systems, but cannot attach itself to other programs. This term should not be confused with the acronym WORM which stands for Write Once Read Many. The WORM acronym is used to define a type data storage device.



THE ATTACK MITIGATOR FROM TOP LAYER
STOPS DoS ATTACKS COLD

Introducing the Attack Mitigator™ from Top Layer. For more information, call 1-888-327-9638, or visit us at www.TopLayer.com

**Top
Layer**™

perfecting the art of network security

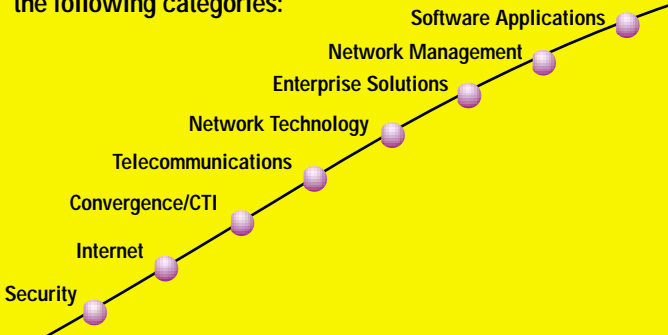
This Technology Guide is one in an ongoing series of over 100 solutions-focused Guides. These Guides assist IT professionals in making informed business decisions about specific aspects of technology development and strategic deployment.

The Technology Guide Series® offers a broad array of titles, each presenting objective information and practical guidance in a non-biased, “easy-to-understand” style and tone. Our editorial writing team has many years of experience in IT and communications technologies, and is highly conversant in today’s emerging technologies.

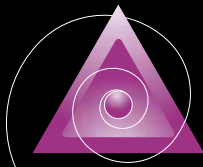
The Technology Guide Series and techguide.com are supported by a consortium of leading technology providers. The Sponsor has lent its support to produce and publish this Guide.

This Guide, as well as the entire Technology Guide Series, is made available to view and print at no charge by visiting techguide.com.

Over 100 Technology Guides in the following categories:



produced and published by



techguide.com

a product of
newmediary®