Unified Threat Management: The Best Defense Against Blended Threats

The SonicWALL® Unified Threat Management solution (UTM) provides the most intelligent, real-time network protection against sophisticated application-layer and content-based attacks and is capable of monitoring a wide variety of network communications, such as e-mail, instant messenger or Web access, on today's highly distributed enterprise.

CONTENTS

Abstract *Threats against computer systems are more than a quarter century old, yet new and complex attacks by hackers continue to wreak havoc on today's connected corporations. For more than two decades, firewall technology—and more recently point solutions such as virus detection and prevention, encryption and patch management—have helped to protect corporate information assets from computer criminals. However, with today's blended attacks—computer network attacks that seek to maximize the severity of damage by combining multiple threat method—these point solutions are no longer sufficient as protective layers. In fact, as the complexity of protective layers increases, new threats become more challenging to defend against as hackers exploit all of the existing protective layers in a blended front. In addition, new targets are continually becoming available as emerging technologies, such as VoIP, become ubiquitous amongst organization's networks. Simple Internet services such as Web access, instant messaging and peer-to-peer file sharing networks (such as Kazaa), already notorious for consuming bandwidth and potentially reducing employee productivity, open up potential security holes.*

Security experts agree that a single weak link in security can compromise an entire security implementation. Therefore, organizations need a unified approach that protects their networks and business users from the threat of blended attacks and technology misuse while decreasing their operating costs. This ever-changing landscape of security threats has made Unified Threat Management (UTM) the fastest growing segment on the security appliance market. UTM refers to a security device that provides broad network protection by combining multiple security features—firewalling, anti-virus, intrusion detection and prevention, and content control and filtering—on a single hardware platform. The UTM acronym was coined by IDC, a prominent global provider of market intelligence, advisory services and events for the information technology and telecommunications industries. Industry analysts note that the rapid rise in blended threats combined with ubiquitous access to information has greatly contributed to a need for the flexible, highly integrated functionality that UTM delivers. The SonicWALL® Unified Threat Management solution (UTM) provides the most intelligent, real-time network protection against sophisticated application-layer and content-based attacks and is capable of monitoring a wide variety of network communications, such as e-mail, instant messenger or Web access, on today's highly distributed enterprise. UTM "intelligence" is an expression of the solution's problem-solving ability; SonicWALL outstrips standard firewall intelligence through the use of a unique multi-layered and unified architecture, delivering a higher level of insight into network traffic and real-time identification of potential breaches or network misuse.

Figure 1. **Ubiquitous Access to Information Leaves Organizations Open to a Multitude of Threats**

A Brief History of Firewalls

For decades, the most basic and important component of any security implementation has been the firewall. Since its invention in the early eighties, the firewall has blocked unauthorized network access. As networking technology has advanced, so has the firewall technology protecting it; evolving from simple access controls based on IP lists to a multilayered system capable of selectively enabling trusted zones while restricting network contagions such as computer viruses.

With the creation of modern networking, which enabled Ethernet-based local area networks (LANs), firewalls came under attack from a new security threat—the Internet worm. To combat this new threat, firewalls were packet-based filters that processed network traffic at very low layers, and compared each packet of traffic to a set of rules defining rudimentary protection based on source and destination of a packet. When the first Internet browsers came on the scene, businesses were able to connect worldwide, and a new generation of firewall technology was needed to create a perimeter defense that validated each network packet against a table of validated network sessions. Soon, firewalls were extended to inspect packets and allow for validation of other security elements.

As networking technologies such as Virtual Private Networks (VPNs) and wireless technology have allowed users to extend the corporate network and remove the dependence on a physical cable for access to the Internet, they have created even bigger strains on network security. While VPN and other new technologies have extended the use of the network, and VPN traffic is encrypted, use of VPN still opens up new potential opportunities for hackers and blended-front viruses to circumvent firewalls. As of 2005, the majority of VPNs still contain exploitable security flaws; this is especially problematic because most VPN users believe the system to be impregnable, so they may be lax around supporting additional security measures. In addition, while VPN empowers users with new points of network access, every new point-of-access provides hackers with another potential point of attack. Despite all of the advances in point solution technologies, the cumulative damage and productivity loss attributed to these new exploits has been devastating, in the hundreds of billions of dollars.

Challenges Facing Today's Corporate Network

Organizations today are struggling with viruses and malicious attacks that are incredibly complex, and are deployed with a multifaceted approach to obtain their desired result. These new blended threats package a combination of virus and worm technology into an extremely elusive attack vehicle. One of the most recent blended threats, myDoom, utilized e-mail as its infection vehicle and delivered a payload that took advantage of millions of computers worldwide to launch a denial of service attack on a target company. It was estimated that in the first five days of the myDoom outbreak, over $60 billion in damage occurred worldwide.

In addition to security threats from blended attacks, administrators also face increased network slowdowns and a lack of prioritization of traffic moving throughout the network that impedes effectiveness. Many of these slowdowns are due to having too many users engaged in non-productive activities such as using Kazaa, peer-to-peer, instant messenger and multimedia applications. While running these types of applications contribute to productivity losses and bandwidth consumption, they also open holes into the internal network for security attacks.

Another challenge for organizations is the increasing use of the Internet for business or personal purposes by internal users. This has given rise to a number of problems associated with lack of control over Internet usage, such as loss of productivity, bandwidth drainage, or legal liability through access to inappropriate or illegal content. Unregulated Internet access can also open the internal network to threats such as spyware, malicious mobile code, key loggers, VOIP attacks, phishing and fraudulent web sites. Access to information must be controlled on a per user basis to maintain the integrity of the network.

To keep their networks updated to address network threats and productivity issues, companies have deployed point solutions and throughout their networks in the hopes of covering all potential threats. One area that IT managers are utilizing point solutions is to protect against internal attacks. According to FBI studies, more attacks are propagated and launched internally than externally. (See Figure 2) Companies are deploying internal intrusion detection systems that place monitors or agents on multiple department segments and e-mail anti-virus systems that prevent viruses from moving. IT administrators also have concerns over threats from remote or distributed environments such as when workers are in a hotel, a HotSpot, or are traveling abroad, and are exposed to threats getting into the corporate network when they

launch a VPN client. To eliminate this threat, organizations are deploying separate VPN solutions for remote users to segment off that traffic from the larger network.

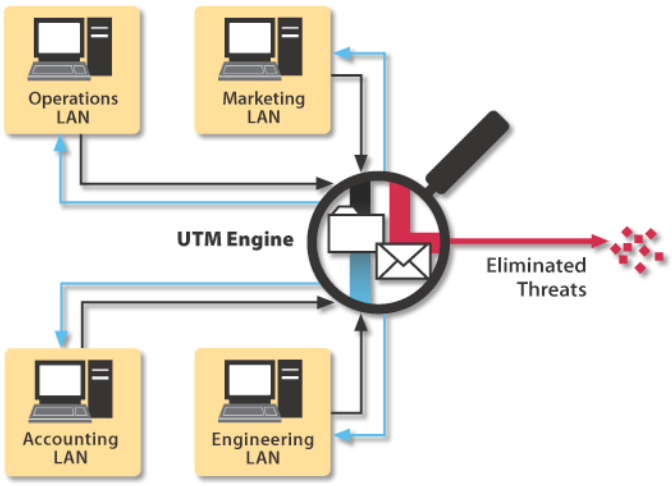

Figure 2**. SonicWALL UTM Blocks Internal and External Threats**

To handle concerns over wireless security, businesses are implementing separate wireless networks to segment out wireless traffic from the internal network and implementing content filtering solutions to decrease productivity issues as well as eliminate spyware. Companies use spam-filters to block out spam, and firewall port-monitoring to restrict viruses. Finally, IT managers are constantly applying patches for servers, workstations, routers, switches and firewalls. While patches can solve issues with existing software, they are often applied too late, or not at all. Proper use of patches requires time-consuming staging and testing, so it is more desirable to forestall the need for patches with patch protection that can be installed at the network level.

While point solutions have proven effective in the past, it's becoming increasingly evident that they do not provide sufficient, timely and unified protection against today's threats. These widespread threats are not only the source of unnecessary financial drain for the modern enterprise, but they but they cause immense productivity losses, and take up an inordinate amount of an IT administrator's time to manage. Point security solutions simply cannot keep up with protecting against these complicated threats and productivity issues, and tend to be difficult to deploy, cannot be managed centrally, and require manual updating, which gives rise to increased operating complexity and overhead costs.

Unified Threat Management – Advanced Security for the Network

Organizations today are looking for an integrated and unified approach to network security—unifying the management of all of these disparate security technologies and productivity technologies into one unit. This is where Unified Threat Management comes in. UTM is an emerging trend in the firewall appliance security market—an evolution of the traditional firewall into a product that not only guards against intrusion—but performs content filtering, spam filtering, intrusion detection and anti-virus duties traditionally handled by multiple systems.

UTM is a compelling and natural consolidation point in the evolution of information asset protection. Part technology and part packaging, it responds to the growing challenge of protecting information assets in the 21st century. Effective unified threat management requires:

Total cost of ownership – Total system costs must be less than the expected loss if there are security breaches due to a lack of controls. The solution must decrease the time to protection and ongoing overhead to achieve a lower total cost of ownership. Security is constantly changing and the system must adapt to these changes on a constant basis with little to no user intervention.

Coordination – Security breaches can occur between mismatched technologies, so when possible, layer your approach to security. Since many threats have multiple attack signatures one layer prevents a portion of an attack, another layer catches the rest. The security posture of the network must adapt in unison for comprehensive protection.

Reduced complexity – to achieve maximum security, solutions must be understandable to implement and components must work well together, or incident detection (and resolution) becomes difficult, if not impossible. Vital considerations include time-to-response and automation of the appropriate protection.

Unified Threat Management addresses these and other requirements by bundling together key information and security functions, and providing simplified administration. Efficiently packaged and effectively delivered, it reduces the cost and increases the reliability of a company's security program.

SonicWALL Unified Threat Management Solution

The SonicWALL complete UTM solution provides the most intelligent, real-time network protection against sophisticated application-layer and content-based attacks available. Comprising Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, this solution flushes out both internal and external threats by addressing multiple threat access points and thoroughly scanning all network layers. Utilizing a high-performance, deep packet inspection engine, SonicWALL delivers threat protection directly on the security gateway by scanning against multiple application types and protocols and by matching files against an extensive signature database.

Many of the point solutions companies' use today utilize a firewall architecture known as stateful packet inspection, which works primarily at the network layer to determine whether data packets were requested and should be allowed onto the network. This approach permits selective but flexible access from outside the network and relatively unrestricted transmission from within. The biggest shortcoming of stateful packet inspection is that it cannot inspect the majority of traffic that passes through it. Also, given that many threats, originate from within an organization's primary technology, such as e-mail, it's clear that numerous threats will bypass the "stateful" level of protection.

SonicWALL employs a comprehensive method known as real-time deep packet inspection *(DPI),* which inspects all network traffic, including encoded, compressed, encrypted and wireless traffic, against an extensive and continuously updated signature database. The SonicALERT team and third party sources work 24x7 to develop up-to-the-minute protection signatures, which are updated on a constant basis to scan in real time and detect and block threats, hidden or not.

With DPI technology, SonicWALL can examine information at the application layer and defend against attacks targeting application vulnerabilities. This DPI engine scans against multiple application types and protocols including SMTP, POP3, IMAP, FTP, HTTP, NetBIOS and dozens of other stream-based protocols, and over 50 application types for intrusion detection and prevention (IDP). The SonicWALL engine scans all network layers including Link, IP, TCP/UDP, Static Ports, and Dynamic Ports and common user applications

such as instant messaging and peer to peer applications—so a company's remote site gateway, internal network, file downloads, servers and desktops are all protected. As an added layer of security, SonicWALL can protect from both internal and external network threats.

SonicWALL UTM provides in-depth insight into network traffic to allow IT administrators continually monitor and improve the effectiveness of their network security. Real-time and historical reports give administrators instant insight into network security status, helping them recognize suspicious activity, assess risks, understand employee behavior and predict future bandwidth needs.

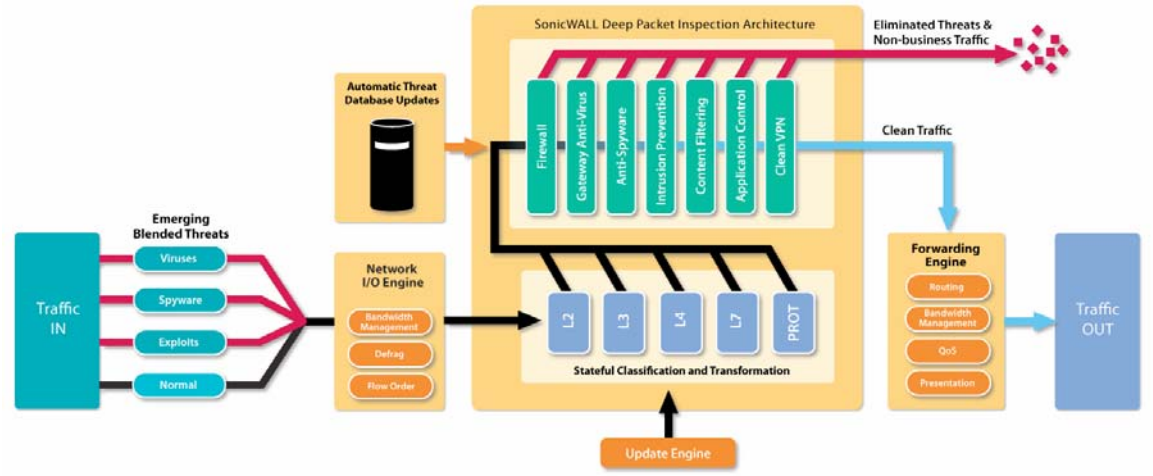

Figure 3. SonicWALL Real-time Unified Threat Management Engine

UTM Solutions Are Not Created Equal

It's clear that companies cannot effectively protect their network from blended threats with the current stateful packet solutions available today. In fact, stateful firewalls only inspect approximately 2% of the traffic that moves through the firewall, while UTM solutions that contain deep packet inspection audit 100% of the traffic. But, even UTM solutions with DPI are not created equal. For example, inside UTM there is "limited" DPI and "comprehensive" DPI. SonicWALL technology is unparalleled in terms of its capacity to handle all users on a network, to scan for threats across all traffic traversing the appliance, and to handle all connections transporting files of any size and most any type. SonicWALL's comprehensive DPI provides the ultimate protection, scalability and performance for today's growing network.

The major differentiator for the SonicWALL UTM engine is that it remains the only solution that is not bound by the requirement to halt and store traffic in memory, a limitation common to all other competitive offerings. The engine can handle scanning of unlimited files sizes and an unlimited number of connections on the network in real time. This scalability and performance is achieved through the utilization of reassembly-free deep packet inspection technology, which has been significantly tuned and designed to enable intelligent inspection at extremely high speed. Unlike other solutions, the SonicWALL UTM technology does not limit the size of file that any one user can download, nor does it limit the number of users that can be protected at one time. Competing offerings give administrators only two options: either passing the traffic unchecked when under excessive load, or blocking all traffic, even legitimate business communication.

The SonicWALL deep packet inspection architecture is by far the most scalable in the industry and the only true, real-time unified threat management solution.

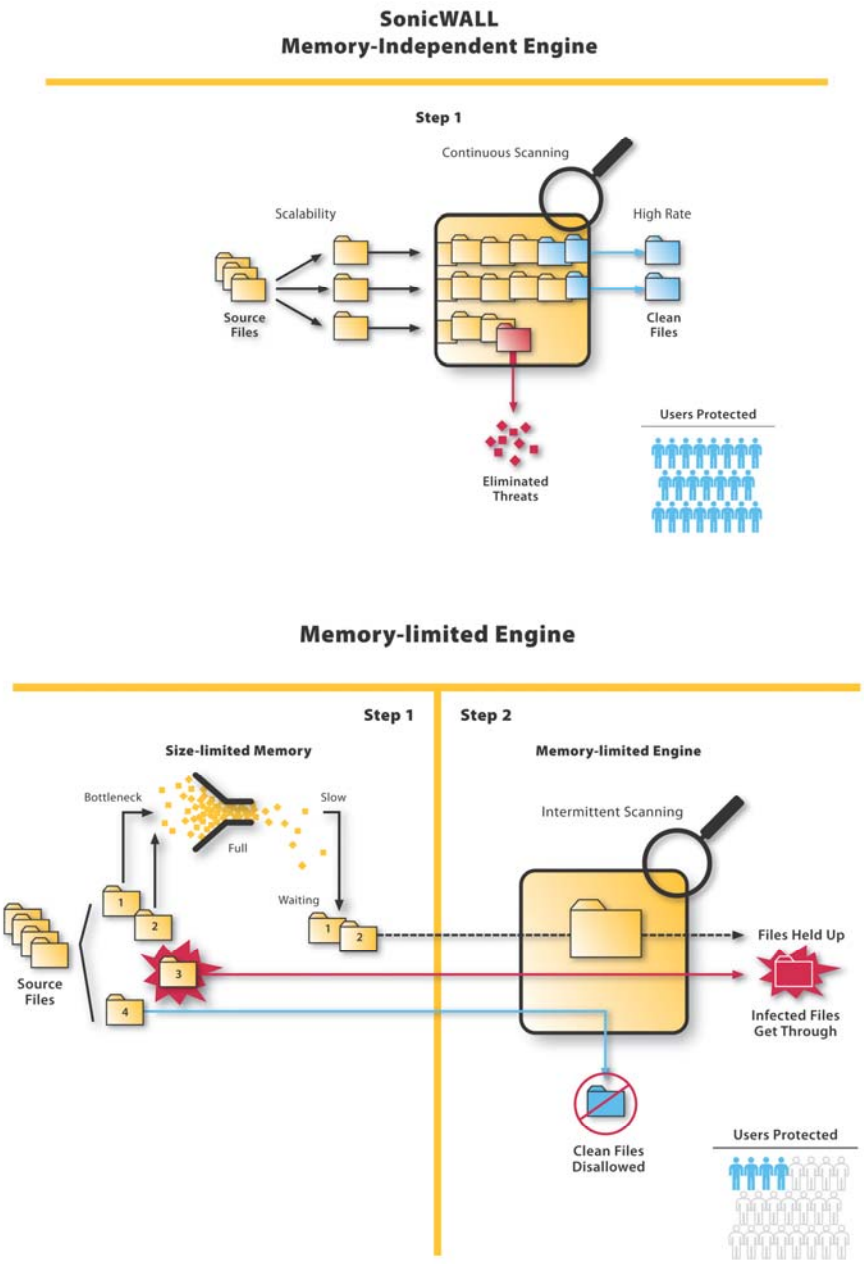

Figure 4. SonicWALL Reassembly-free Deep Packet Inspection Technology

Future-proofing the Corporate Network

New threats that emerge daily, such as viruses and spyware infect present an ever-present nightmare for administrators to stay current with security updates to networks and systems. Some have the ability to spread within hours and affect computers and networks of all sizes. As these attacks become more dynamic and malicious in nature, businesses are forced to look at unified threat solutions that will protect them without the need for manual intervention, not only against current threats, but emerging threats

Unlike other UTM solutions, SonicWALL Unified Threat Management is designed to respond to new threats as they appear. It's a continually adapting security appliance that changes its security posture pro-actively to protect the network against the latest emerging threats—whether they come from the overseas, next door or inside the network. Most importantly, continual threat updates require zero administrator intervention, offering an automated and proactive approach to remaining protected.

It's a future-proofing and adaptable appliance that's good for today, tomorrow and next year.

Significant ROI

The SonicWALL UTM solution is designed to decrease administrative costs in both threat prevention and security. By having an integrated security solution, an administrator can leverage the SonicWALL team of security experts who continuously develop new protection technologies to proactively protect business networks. This decreases an administrator's costs, delivers better return on investment, and increases productivity by ensuring that sensitive data in not compromised, reliable communication is achieved, Web resources are being used appropriately, and networks don't slow down due to inappropriate applications and traffic. SonicWALL UTM relieves these pressures and challenges from the network. SonicWALL unified threat architecture is by far the most scalable in the industry and the only true, real-time unified threat management solution.

SonicWALL solutions are also affordable for organizations of all sizes—from the smallest organization to the largest—providing the most secure network capabilities available anywhere.

Summary

Security for computer networks has come a long way from the advent of firewalls in the early eighties. Yet, with the complexity of attacks ever changing in sophistication and speed, security has never been more important. While existing point solutions were once effective at protecting corporate networks, they no longer suffice as individual protective layers. Today, corporations need a distributed and effective front against the modern threats facing information networks – they need unified threat management.

SonicWALL Unified Threat Management uses a highly scalable, reassembly-free, deep packet inspection architecture—deep packet inspection and unified threat management architecture that looks for viruses, worms, Trojans, spyware and emerging threats to VoIP traffic—providing threat protection directly on the security gateway. By incorporating content control and filtering for Internet services such as web access, instant messaging and peer-to-peer file sharing use, productivity can be increased and legal liability risk is minimized.

The SonicWALL UTM architecture is continuously updated by a team of signature writers who work around the clock to develop protection techniques to the latest vulnerabilities that occur with operating systems and networks and control for the use of common user applications. SonicWALL UTM makes sure that the security posture in each one of an organization's locations, whether that be a large corporate site, small remote, via a telecommuter or branch office sites is delivered without any user intervention for complete protection against today's latest threats. It offers complete support for all users, whether they are at an enterprise site or in-between network zones—allowing unlimited file sizes to move through the firewalls and ensuring maximum protection.

The compelling SonicWALL combination of innovative technology, high performance, cost-effectiveness and reliability garnered the Grand Prize in the Network Security category at Interop Tokyo 2005—the premier forum for telecommunications and network technology. It's no surprise then that SonicWALL has emerged as the worldwide leader in Unified Threat Management, helping companies defend against network attacks, improve productivity and efficiency, simplify administration through a single management interface and lower the total cost of network security ownership.