Denial of Service Attacks:

An Emerging Vulnerability for the "Connected" Network

A White Paper prepared by SonicWALL, Inc.

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
1-888-557-6642
http://www.sonicwall.com

Overview

Increasingly, the types of attacks facing Internet-connected networks are geared at denying access to essential services by legitimate users – often by crashing servers or routers, or by overwhelming the network with enough traffic to degrade service. This is a change from the past, when many attacks were carried out to gain access to confidential data.

These Denial of Service Attack (DoS) attacks are relatively easy to execute, and are made even easier by the online hacking and, ironically, security communities. Online resources archive utilities that anyone can download. Technical aptitude is no longer required to launch a DoS attack; all it takes is a readily available software program and a target network.

This white paper discusses common DoS attacks, as well as how the SonicWALL Internet Security Appliance protects against such attacks.

TCP/IP 101 - How IP Works

Computers share information over the Internet using a common language called IP (short for "Internet Protocol"). IP, in turn, is a set of application protocols that perform specific functions. These protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc., are also identified by number, called the "TCP port" or "UDP port". For example, Web traffic typically uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific IP port for requests for information from remote client computers on the network. For example, a Web server typically listens on port 80. It is important to understand that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
137-139	NETBIOS

Television may be used as a loose analogy. Multiple TV programs are simultaneously sent over a single media (cable, air, etc.). The desired program is received by tuning the TV to "listen" to the correct frequency, or channel. The other channels are still broadcasting on that shared media, but the TV ignores them and only displays the program on the desired channel. What is happening on the other channels that are not being watched? There is no way to know.

That is the problem for computers with an unsecured connection to the Internet: there is no way to know what is happening to the computer over the "unwatched" ports. A function of firewalls is to block access to network services over unwatched ports.

Port Scans

To discover these unwatched ports on the target, hackers often employ a technique called "port scanning".

There are more than 130,000 IP ports, many of which have clearly defined purposes, such as port 21 for FTP, 23 for Telnet, 25 for SMTP, 80 for HTTP (Web), and 110 for POP3. However, other ports may be used for tasks. Port 389, for example, is often used for LDAP directory access and port 8080 for a test Web site.

Readily available port scan applications attempt to connect to a computer by trying all IP ports on that host. Any response that indicates an open connection is put in a log for the initiator of the port scan to investigate. An analogy to a port scan would be a burglar who "cases" a neighborhood by checking all houses for unlocked doors and windows. It is essential that any Internet-connected organization be protected from port scans, which usually appear in the early stages of a sophisticated attack.

In general, a port scan will look like a series of "TCP Connection Dropped" or "UDP Connection Dropped" log messages. During the course of a port scan, the log will show the destination IP address is the same, but the destination IP port number will change. While most port scanning tools will attempt to connect over sequential IP ports, that is not always the case as some will randomize the ports to avoid easy detection.

The following section of log from SonicWALL illustrates how a port scan may appear.

```
[…]
04/20/1999 03:54:22
TCP connection dropped
Source:146.87.218.182, WAN
Destination:209.125.234.84, 22, LAN

04/20/1999 03:54:41
TCP connection dropped
Source:146.87.218.182, WAN
Destination:209.125.234.84, 23, LAN

04/20/1999 03:55:00
TCP connection dropped
Source:146.87.218.182,, WAN
Destination:209.125.234.84, 24, LAN
[…]
```

From this section of the log, it is apparent that the computer with the IP address 146.87.218.182 is scanning ports

on the server with the IP address of 209.125.234.84.

SonicWALL's default behavior is to block all connections that originate from the Internet. Unless the SonicWALL has been configured to allow specific types of traffic into the LAN, port scans are not a threat as attempts to connect to all machines on the protected network will be blocked by the firewall.

IP Spoofing

Since hacking is considered a criminal offense, many hackers employ a technique known as "IP Spoofing" to hide their identity. This is done by modifying IP packet headers to look like they come from a different computer.

IP Spoofing may also be used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. For example, IP spoofing is used to easily thwart security measures that use only simple packet filtering and/or Network Address Translation (NAT). IP Spoofing may also be used to magnify the effect of a DoS attack, as is the case during a LAND attack.

Many firewalls are unable to detect IP spoofing. For those firewalls that are able to detect and log the connection using spoofed addresses, the log information is not directly useful in finding the culprit because the source address has been changed. However, with the help of the ISP, it is possible to trace the attacker during the course of the attack.

The following is a SonicWALL log entry showing a blocked attempt to connect to a server on the DMZ port using a spoofed IP address.

```
04/20/1999 21:00:16
IP spoof detected
Source:209.19.28.50, 3356, WAN
Destination:209.19.28.84, 80, DMZ
```

SonicWALL is pre-configured to block and log all attempts to access the protected network, including the DMZ port, using spoofed IP addresses. A DMZ port ("De-Militarized Zone") is used to give Internet users access to public servers, such as Web, FTP, and E-commerce servers, while providing some level of firewall protection. In the case of SonicWALL, servers on the DMZ port are protected from DoS Attacks. SonicWALL also sends an immediate alert message to the administrator when IP spoofing is detected.

Denial of Service Attacks

There are three types of DoS attacks: those that exploit bugs in a TCP/IP implementation, those that exploit weaknesses in the implementation of TCP/IP, and brute-force attacks that flood a network with useless data.

It is important to understand that the disruption of servers and services caused by the DoS attack may be the actual

goal of the attacker, or may be a prelude to a more sophisticated attack. For example, an automated system may attempt denial-of-service attacks on consecutive groups of IP addresses, and then ping them for a response. If there's no response from a downed server (and thus the denial-of-service attack was apparently successful), the site may be targeted for more sophisticated hacking at a future date.

TCP/IP Implementation Bugs

"Ping of Death", and variants such as "Teardrop", "Bonk", "Nestea", and similar attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

Ping of Death attacks exploit weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Ping of Death program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

SonicWALL drops all malformed IP packets. This behavior does not cause a problem as malformed packets can not be used for normal communications and would be dropped by those machines on the network that don't crash when these packets are encountered.

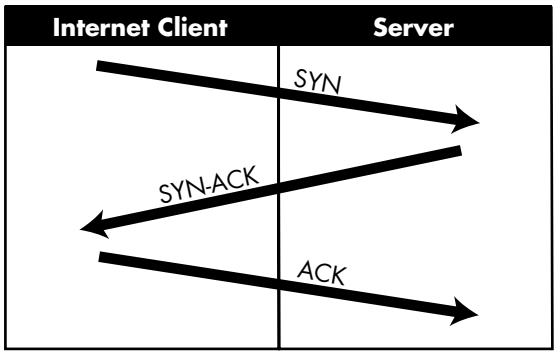
SonicWALL's alert and log message will be similar to the following, showing the computer with the IP address 12.76.68.52 is sending a Ping of Death to the DMZ computer with the IP address of 209.125.234.83:

```
04/20/1999 21:10:36
Ping of death blocked
Source:12.76.68.52, 8, WAN
Destination: 209.125.234.83, DMZ
```

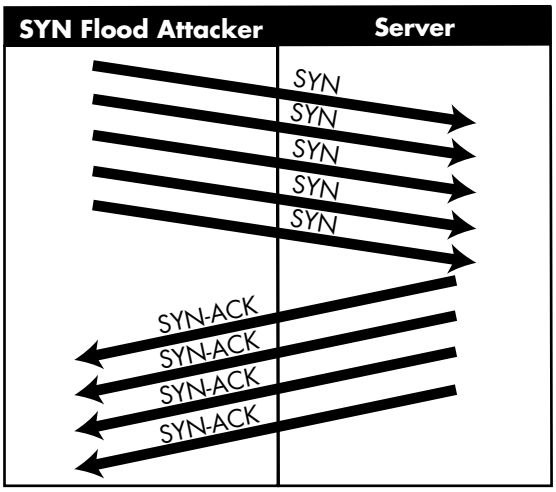
SonicWALL also sends an immediate alert message to the administrator when a Ping of Death is detected.

TCP/IP Weaknesses

Weaknesses and bugs in the implementation of TCP/IP leaves it open to "SYN Flood" and "LAND" attacks. These attacks are executed during the handshake that initiates a communication session between two applications. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving application. The receiver sends back a SYN-ACK (acknowledgment) packet, and then the initiator responds with an ACK (acknowledgment). After this handshake, the applications are set to send and receive data. This process is shown below.

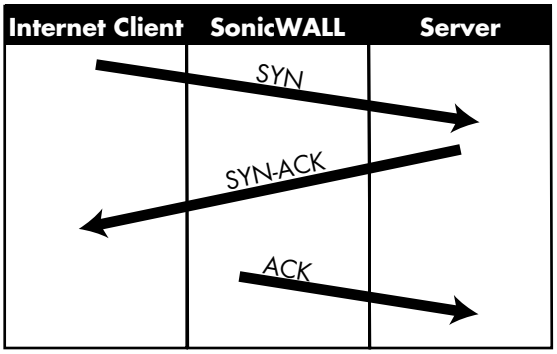


During a SYN Flood attack, the targeted system is flooded with a series of SYN packets, shown below. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.



In a LAND Attack, hackers send one or more SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

SonicWALL protects against SYN flood attacks by completing the final "ACK" for the remote host, as shown below. SonicWALL then monitors the session and resets the connection should the remote computer fail to request data.



Normal activity on the Internet can create the appearance of a SYN Flood attack because the final ACK may be lost in transmission. SonicWALL will log SYN Floods as "Possible" and "Probable". Attacks that are listed as "Possible" may be deliberate attacks, or may be symptomatic of clients with connectivity problems. When a SonicWALL alert and log message show the SYN Flood as "Probable" it is most certainly a deliberate attempt to crash or disable the target.

The following is a SonicWALL log entry showing a SYN Flood attack that was blocked.

```
04/20/1999 17:44:44
Probable SYN flood attack
Source:199.88.110.27, 1219
Destination:209.125.234.83, 80
```

This section of the log shows the computer with the IP address 199.88.110.27 is sending a SYN flood to the DMZ computer with the IP address of 209.125.234.83 over IP port 80 (HTTP).

SonicWALL is pre-configured to block and log all SYN Flood attacks. SonicWALL also sends an immediate alert message to the administrator when a SYN Flood is detected.

WinNuke

WinNuke is a program whose sole function is to crash any unprotected Windows computer on the Internet. WinNuke crashes a PC by sending illegal data to any IP port that listens for data on a Windows PC. IP port 139, used by NetBIOS (Windows networking) seems to be the most common.

When a PC has been "WinNuked", it will crash into a blue screen with the following text:

```
Fatal exception 0E at 0028: in VxD MSTCP(01) + 000041AE.
This was called from 0028: in VxD NDIS(01) + 00000D7C.
```

A reboot usually fixes whatever damage the WinNuke attack causes.

During a WinNuke attack SonicWALL's log will contain "TCP packet dropped" messages, similar to the following.

```
04/20/1999 22:36:44
TCP packet dropped
Source:199.88.110.27, 4365
Destination:209.125.234.83, 139
```

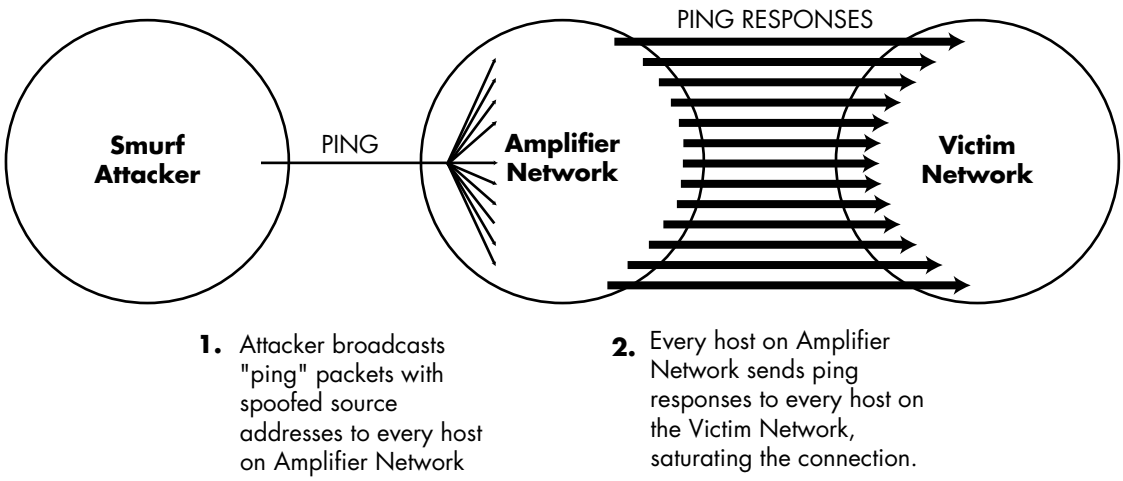
Note that port 139 is used in the course of normal network activity. The existence of these messages does not mean that a WinNuke attack has occurred.

SonicWALL's default behavior is to block all connections that originate from the Internet. Unless the SonicWALL has been configured to allow specific types of traffic, such as IP port 139 into the LAN, WinNuke attacks are not a threat as attempts to connect to all machines on the protected network will be blocked by the firewall.

Brute-Force Attacks

A bandwidth attack, such as a "Smurf" attack, targets a feature in the IP specification known as "direct broadcast addressing" to quickly flood the target host or network with useless data.

A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). The hacker sets the destination IP address of each packet to the broadcast address of the network, causing the router to broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "amplifier" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible. A Smurf attack is illustrated on the following page.



Smurf attacks are run over extended periods of time. SonicWALL's log will be filled with hundreds or thousands of "ICMP packet dropped" messages when the protected network is used as the amplifier network. The source address will be the spoofed address of the amplifier network, for example:

```
04/20/1999 17:44:44
ICMP packet dropped, 0
Source:199.88.110.27, 1219
Destination:209.125.234.83
```

SonicWALL protects against being the amplifier network by dropping all traffic that is initiated from the Internet. Since the attack actually targets the connection "upstream" of the victim network, there is no way for a firewall to protect against a Smurf attack. The best measure is to immediately notify the ISP and hope they are able to identify and stop the attacker or the amplifier network.

Who is attacking you?

Firewalls that are able to detect and thwart DoS attacks will typically log the attack. For example, the following is the SonicWALL log entry for an actual Ping of Death attack:

```
04/20/1999 21:10:36
Ping of death blocked
Source:12.76.68.52, 8, WAN
Destination: 209.125.234.83, DMZ
```

The first thing to do is determine where the attack is coming from. There are several tools that will do this, the most common of which is "Whois". Whois is a UNIX command which is run from a Telnet window to a "shell" account and pointed to the Whois server at "whois.arin.net". If you do not have access to a shell account, shareware and freeware programs, such as "Cyberkit" for Windows from < http://www.ping.be/cyberkit/download.html>, or "WhatRoute" for Macintosh from <http://crash.ihug.co.nz/~bryanc/> can be used.

The Telnet command is: whois -h whois.arin.net <Attacker IP Address>

For example, the command: `whois -h whois.arin.net 209.19.28.83`

Results in:

```
Big ISP (NETBLK-BIGISP) BIGISP2
209.19.0.0 - 209.19.255.255
Owner Network (NETBLK-BIGISP-OWNERNET1) BIGISP-OWNERNET1
209.19.28.80 - 209.19.28.95
```

These results show that "Big ISP" has assigned the block of addresses 209.18.28.80 to 209.19.28.95 to "Owner Network". The first text after that in parentheses, in this case "BIGISP-OWNERNET1" is the handle used to find who manages "Owner Network".

The Telnet command is: whois -h whois.arin.net <Handle>

For example, the command: `whois -h whois.arin.net BIGISP-OWNERNET1`

Results in:

```
Owner Network (NETBLK-BIGISP-OWNERNET1)
    123 Main St.
    Anytown, CA 95123
   US

    Netname: BIGISP-OWNERNET1
    Netblock: 209.19.28.80 - 209.19.28.95

    Coordinator:
   Smith, John   (JS100-ARIN)   jsmith@OWNERNET.COM
     555-555-1212
```

What Should You Do?

What should you do when your network is under attack? Opinions vary widely, from "report everything", to "report nothing, SonicWALL blocked it anyway." Also remember that the address of the attacker may be spoofed, and who appears to be the attacker, is actually innocent.

Most people ignore transient scans where a user briefly scans or attempts to connect to a port. If the same user keeps

retrying the same port over an extended period of time, it may be wise to notify the user's ISP about it.

It is wise to report all port scans. Consider that an attempted "attack" and report it.

Immediately report Smurf attacks to your ISP.

As a general rule, attacks can be reported via E-mail to <abuse@isp.address> or <postmaster@isp.address>. Also, cc: the person shown as responsible for the network. When reporting an attack, make sure to include all log information. If you do not receive a response, call the person responsible for the network; it is possible that their network security has been compromised and the hacker is intercepting the warning E-mail messages.

About SonicWALL

Many firewalls require manual configuration, or the installation of "patches", to protect them from DoS attacks such as Ping of Death, SYN Flood, LAND Attack, IP Spoofing, etc. Others are not able to protect the network, or even themselves, against DoS attacks.

The SonicWALL Internet security appliance is pre-configured to automatically detect and thwart all known DoS attacks. As the hacker community develops new DoS attacks, SonicWALL aggressively works to develop upgrades to thwart these new attacks. SonicWALL's "**Auto Update**" mechanism automatically notifies the SonicWALL administrator via E-mail when a new version of firmware is available on SonicWALL's FTP site which contains new DoS attack prevention updates. This is a free service offered to all registered SonicWALL customers.

The SonicWALL Internet security appliance is also available in three models to best suit the needs of the organization it is protecting.

- **SonicWALL SOHO** is a secure and affordable way to protect small networks, such as those using cable modems or DSL, from theft, destruction, and manipulation of critical business or personal data. SonicWALL SOHO's IPSec VPN option makes it the perfect solution for corporate telecommuters and small remote offices. SonicWALL SOHO/10 supports 10 nodes on the LAN. SonicWALL SOHO/50 supports 50 nodes on the LAN.
- **SonicWALL DMZ** is ideally suited for the Internet security needs of K-12 schools, larger business networks, and e-commerce applications. SonicWALL DMZ supports an unlimited number of nodes on the LAN, and includes a DMZ port ("De-Militarized Zone") to allow Internet users to access public servers, such as Web, FTP, and E-commerce servers, while providing DoS Attack prevention.
- **SonicWALL PRO** provides Internet security, Virtual Private Networking (VPN), and content filtering with high performance hardware to meet the needs of large, Fast Ethernet networks. SonicWALL PRO offers branch offices, intranets, and large, single-site networks a comprehensive security system to combat intruders and secure important business data.

SonicWALL Model	Nodes	VPN	Enterprise Features	DMZ Port	10/100 Ethernet Ports
SonicWALL SOHO/10	10	Optional	Included		
SonicWALL SOHO/50	50	Optional	Included		
SonicWALL DMZ	Unlimited	Optional	Included	Included	
SonicWALL PRO	Unlimited	Included	Included	Included	Included

All members of the SonicWALL family offer:

- **Firewall Security.** SonicWALL uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. Stateful packet inspection is similar to the algorithms used by enterprise level firewall vendors, such as Check Point and Cisco, and is widely considered to be the most effective method of protecting the private LAN.
- **Hacker Attack Prevention.** SonicWALL is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack, IP Spoofing, etc. The goal of a DoS Attack is not to steal information, but to disable a device or network so users no longer have access to network resources. For example, "WinNuke", a widely available DoS tool, is used to remotely crash any unprotected Windows PC on the Internet; SonicWALL protects the private LAN from WinNuke and many other DoS attacks.
- **IPSec VPN.** SonicWALL VPN provides an easy, affordable, and secure means for businesses to connect all offices and partners together. Using data encryption and the Internet, SonicWALL VPN provides secure communications between multiple sites or hundreds of remote users. Encryption methods include 168 bit Data Encryption Standard (Triple-DES), 56 bit Data Encryption Standard (DES) and 56 bit ARCFour (ARC4). SonicWALL VPN can be used with other VPN products with the same IPSec implementation, such as Check Point's FW-1. A single-user license remote access VPN client for Windows is also included to allow secure remote management. Multiple VPN client licenses are available to provide remote LAN access for the SonicWALL PRO.
- **Internet Content Filtering.** Content filtering allows businesses and schools to create and enforce Internet access policies tailored to the needs of the organization. An optional Content Filter List subscription is available which allows the administrator to select categories of Internet sites, such as pornography or racial intolerance, to block or monitor access. Automatic weekly updates of the customizable Content Filter List make sure that access restrictions to new and relocated sites are properly enforced. Users may be given a password to bypass the filter, giving them unrestricted access to the Internet.
- **IP Address Management.** Network Address Translation (NAT) allows companies to use private addresses for

security and easier address management. NAT also allows SonicWALL to support LANs using low cost Internet accounts, such as xDSL or cable modems, where only one IP address is provided by the ISP. DHCP Server and Client provide centralized management of TCP/IP client configurations and the ability to acquire TCP/IP settings from the ISP.