



Pioneering Technologies
for a Better Internet

Cs3, Inc.

5777 W. Century Blvd.
Suite 1185
Los Angeles, CA 90045-5600

Phone: 310-337-3013
Fax: 310-337-3012
Email: info@cs3-inc.com

The Reverse Firewall: *Defeating DDOS Attacks* *Emanating from a Local Area Network*

(Patent Pending)

Abstract

Firewalls protect networks from incoming packets. In contrast, the Reverse Firewall protects the outside network from packet flooding Distributed Denial of Service (DDOS) attacks that originate on the inside. The Reverse Firewall drastically reduces the impact of DDOS attacks mounted from inside the network. DDOS attacks are usually conducted through "zombies" -- computers that have come under the control of the attacker. The Reverse Firewall chokes off packet flooding attacks before they exit the network where they originate. This paper describes the Reverse Firewall, how it works, and its benefits as a DDOS defense to the infrastructure owner and to the Internet.

Contents

- [1. Packet Flooding DDOS Attacks](#)
 - [2. Existing Solutions](#)
 - [3. The Reverse Firewall](#)
 - [4. Benefits and Costs of the Reverse Firewall](#)
 - [5. Reverse Firewall Deployment Issues](#)
-

1. Packet Flooding DDOS Attacks

Denial of Service (DoS) and Distributed DoS (DDoS) packet flooding attacks are an increasing problem. A recent study estimates over 4000 attacks a week (See [details about the study](#)). Many sites of commercial importance have become targets, including CNN, EBay, Yahoo, and Microsoft, establishing DDOS attacks as a serious threat to e-commerce and e-business. The Computer Emergency Response Team (CERT), the Internet security watchdog, was itself targeted in successful DDoS attacks in March 2001. CERT warns repeatedly that there is currently no technology to deal with this problem and recommends general vigilance and administrative measures to minimize the potentially devastating impact of a DDoS attack.

The Internet infrastructure has vulnerabilities that make it very difficult to defend against packet flooding attacks. Please see the White Papers entitled "[IP Changes to Eliminate Source Forgery](#)" and "[A Fair Service Approach to Defending Against Packet Flooding Attacks](#)" for more detailed analysis of infrastructure vulnerabilities that make DDOS an extremely challenging problem to solve.

Most DDOS attacks are carried out via "slaves" or "zombies", machines that have been compromised, and come under the control of the attacker(s). Using these machines, the attacker can launch a coordinated but well-disguised attack on a victim and avoid detection. With near universal availability of permanent and faster connections to the Internet, and with the attendant decrease of network security expertise per individual computer, there is no scarcity of potential zombies. All ISPs, Universities, and owners of infrastructure must be concerned about their computers being used in this fashion.

2. Existing Solutions

There is no deployed technology that has successfully defended against DDOS attacks. Most of the approaches focus, perhaps understandably, on protection of customer sites against incoming attacks. This turns out to be very difficult to do with today's Internet architecture and protocols (see [related paper](#) for a more complete analysis of these issues). The [WWW Security FAQ](#) describes useful administrative procedures that are "best practices" to combat DDOS attacks. Several startups are working on developing DDOS defense technology based on smart filtering of incoming packets at ISPs and upstream routers (See [a recent technology survey](#) in InfoWorld). Cs3 is advocating protocol changes that fix the fundamental flaws of the Internet -- such as IP source address forgery.

There are two current forms of defense that have at least some utility in preventing attacks that originate from a local network. These are both universally recommended and hardly ever actually used in practice! These are:

- **Prevention of Zombie-Infestation:** Computer owners are encouraged to keep up to date on software patches in order to prevent the exploitation of widely known vulnerabilities. [Intrusion Detection Systems \(IDS\)](#) can sometimes alert network administrators to the fact that their systems are in imminent danger, or have recently been compromised. There are several scanning tools that search for known "malware", such as attack scripts and viruses.
- **Ingress Filtering:** ISPs should refuse to forward packets with clearly invalid IP source addresses. This has been widely recommended for years but still seems rare.

We advocate both of these. They both have substantial benefits apart from preventing flooding attacks from originating within a network. Unfortunately, although they do help, they do not actually solve this
Cs3, Inc. *Page 2* [The Reverse Fire-Wall](#)

problem. The first is similar to virus scanning. There are always new vulnerabilities. All an administrator can do is try to defend against the ones that have been recognized and patched. This can also absorb as much effort as the administrator is willing to expend, so even the best protection is a tradeoff between cost and benefit. Furthermore, this approach is possible only to the extent that the owner of the local network actually controls the hosts inside. This works well for a corporate network, less so for an academic network, and not at all in the case of an ISP.

The second approach happens to be very useful against the most prevalent packet flooding attacks currently in use, since these tend to randomize the source addresses of the attack packets. This makes it harder for the victim to find the origin of the attack packets. However, source address filtering does not prevent the attack. If more providers start filtering impossible source addresses then the attacks will simply stop relying on this vulnerability.

3. The Reverse Firewall

A traditional firewall protects a network from incoming packets. What makes the Reverse Firewall a unique device is that it protects the outside from packet flooding attacks that emanate from within the network. This is particularly useful for all owners of Internet infrastructure providing Internet connectivity. Such entities include:

- ISPs : that offer high speed Internet access to customers via dedicated network connections such as DSL and cable.
- Universities : that provide computers for use within the campus community, along with high-speed Internet connectivity for those computers. Often, members of the community maybe allowed to connect their own computers to the high-speed campus network.
- Corporate networks : provide Internet connectivity to workstations that are used by employees. Corporations generally have a great deal of control over the machines in their networks.

The Reverse Firewall works by filtering the outgoing packets from a network. The difference between a legitimate application that uses high bandwidth and a packet flooding attack is that in the former case the machine at the other end of the conversation is participating in a two way conversation, whereas the attack is one sided. [[See note on attacks using two way conversations](#)] Unlike other network infrastructure, a firewall is in a position to distinguish these two cases, since all of the traffic between the local network and the outside (the Internet) passes through it.

What we call a Reverse Firewall is, therefore, simply one part of the functionality that could and should be provided by firewalls. All it does is limit the rate at which it forwards packets that are not, in some sense, replies to other packets that recently were forwarded in the other direction. Of course, it must be possible to send SOME packets that are not replies, for instance to start a new conversation. But such packets need not be transmitted at a high rate.

The machines of greatest value to attackers are those with fast Internet access, because it is from these machines that they can send packet floods at very high rates. The Reverse Firewall reduces the value of these machines for such an attack to that of a slow dial up connection, or even less. Attackers currently try to amass collections of hundreds or thousands of zombies from which to attack simultaneously. The Reverse Firewall, however, reduces the effectiveness of a zombie by a similar factor!

4. Benefits and Costs of the Reverse Firewall

Most infrastructure owners trust their users not to mount packet flooding attacks, but this does not eliminate the problem. As described earlier, it is much more likely that some hosts inside a local network will be taken over by remote hackers for use as zombies in coordinated DDOS attacks.

While DDOS attacks are mainly targeted at a victim outside the infrastructure provider's local network, they are, in fact, also attacking the legitimate users of the local network infrastructure. In particular, the attacker is using up as much of the outgoing bandwidth as the zombie machines can consume. This is bandwidth that is therefore no longer available to other legitimate users of the network. Furthermore, if upstream providers charge for actual network usage (rather than a flat rate), the attacker is actually directly increasing the costs to the network owner. By using the Reverse Firewall appropriately (see [discussion on deployment](#) for details), the infrastructure owner gains the tangible benefit that attacks from one network segment cannot disrupt customers from other segments.

As DDOS attacks increase in frequency and impact, perceptions about the responsibilities and liabilities of being an infrastructure owner are shifting. There is understandable pressure on infrastructure owners to be more diligent and proactive in ensuring that they are not unwitting hosts of lethal DDOS attacks. The Reverse Firewall is a tool with which the infrastructure owner can accomplish that goal.

The Cs3 Reverse Firewall approach (rate limiting of unexpected packets and the use of fair scheduling by places) is inherently superior to existing solutions that do scanning for known attack script signatures on potential zombie computers because it requires no updates as attackers change their methods and level of sophistication.

5. Reverse Firewall Deployment Issues

Most commercial entities are understandably interested in protecting their own infrastructure from becoming the targets of DDOS attacks. Interestingly, the Reverse Firewall functionality is actually completely symmetric with respect to incoming and outgoing traffic. In other words, it does protect the local network from the outside in the same way that it protects the outside from the local network. Unfortunately, this is not adequate to defend the local network from the outside.

This is related to the fact that the outside is normally much bigger than the inside. It is true that large numbers of attack packets from the outside will be stopped at the network's firewall. But this is too late to protect the communication between the inside and the outside. The problem is that, during a packet flooding attack, most of the packets that legitimate customers send to the victim will be lost long before they reach the victim's firewall. As a result, a comprehensive DDOS defense will require more major infrastructure changes (please see [related papers](#) for a detailed analysis of the changes that Cs3 strongly advocates). In fact, the larger the network owned by infrastructure providers, the more beneficial it will be for them to incorporate these additional features within their network infrastructure to protect themselves and the outside.

How many Reverse Firewalls does an infrastructure owner need? This is a cost/benefit tradeoff. One firewall can handle the traffic from a large number of machines. However it can only stop the attack traffic that flows through it. In order to prevent one internal machine from denying service to another, the two have to be separated by a firewall. In fact, the same Reverse Firewall can be used to protect different internal network segment from one another by connecting each network segment to a different network

interface card in that firewall. Such a firewall would not only protect the inside network from the outside network and vice versa, it also protects the different internal segments from one another.

As an example, it is reasonable that, for a University network, one might install a separate Reverse Firewall (or separate network interface card as discussed above) for each dormitory or department. Then a zombie in the Physics department, for example, would affect only the Physics department and not the rest of the campus. If it is important to prevent an attack originating in one part of the Physics department from affecting another part, then those two parts must be separated and given different firewalls. Such reasoning is applicable for ISPs, Universities, and all other infrastructure owners who have limited control of the hosts on their network.

6. Implementation Status

Cs3 is developing this technology using funding from Defense Advanced Research Projects Agency (DARPA) and the California Technology Investment Partnership (CAL TIP). A Linux Reverse Firewall is now available for external use and testing. A freeBSD version is targeted for release this Fall. The Reverse Firewall mechanism is available on a licensing basis to commercial firewall vendors.

6. End Notes

End Note 1: Using Two-Way Conversations

One might object here that it is also possible to use up the victim's bandwidth by downloading large files, etc. We regard this as a very different sort of attack, since it requires the actual cooperation of the victim - - DDOS attacks generally do not. In fact, infrastructure owners can control their legitimate connections and we believe they should. So should the victim. If the attack is limited to legitimate connections, the victim is at least as much to blame for allowing the attacks to occur as the infrastructure provider.

[Back to Reference](#)