

Defense Against the DoS/DDoS Attacks on Cisco Routers

by: Hang Chau, 09/17/2004

<http://www.securitydocs.com/library/2553>

Abstract

DoS/DDoS attacks are a virulent, relatively new type of Internet attacks, they have caused some biggest web sites on the world -- owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon -- became inaccessible to customers, partners, and users, the financial losses are very huge. On the other hand, if the international terrorist organizations use the DoS/DDoS to attack successfully the web sites or Internet systems of U.S. government and military, the results and losses will be disastrous and unimaginable.

Cisco routers are said to have a market share of over 90% in the Internet. They are used widely by most large companies and agencies all over the world, and are considered as the most important building blocks of the Internet. But, Cisco routers have several vulnerabilities that could allow hackers to disrupt Internet traffic, intercept sensitive information such as passwords and credit card numbers or redirect traffic from web sites. Securing the router is the first thing that network administrators need to do.

Therefore, for guarding both American national security and commercial security, it is really important to detecting, preventing and mitigating the DoS/DDoS attacks on the Cisco routers.

1. Introduction

DoS/DDoS attacks are a virulent, relatively new type of Internet attacks, they have caused some biggest web sites on the world -- owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon -- became inaccessible to customers, partners, and users, sometimes for up to twenty-four hours; some web sites have experienced several days of downtime while trying to restore services, the financial losses are very huge.

From a latest important report "2003: CSI/FBI [1] Computer Crime and Security Survey", we know the following information about the DoS/DDoS attacks in America:

1. 42 percent of respondents of the survey suffered the Denial of Service (DoS) attacks (from 1999 to 2002, only 27-40 percent of respondents suffered the DoS attacks).
2. 111 of 398 respondents reported the financial losses caused by the DoS attacks.
3. The total losses by DoS attacks was over 65 million US dollars, or average losses 1.427 million dollars, it is the 4.8 times of average losses on 2002 (from 2000 to 2002, the average losses caused by the DoS attacks are only 0.108, 0.122, 0.297 million dollars respectively).
4. In "WWW Site Incidents: What Types of Unauthorized Access or Misuse", 35% are Denial of Service attacks.
5. In addition, on the 2001's version of the CSI/FBI Survey, when the DoS attacks increased by an astonishing 33 percent on network, where firewalls had been installed in 90 percent of instances.

DoS/DDoS attacks are also easy to launch. For example, a teenager using very simple DoS tools managed to cripple the web sites of large E-Commerce companies like Yahoo and Amazon, during a series of DoS/DDoS attacks in February 2000 [2].

Cisco routers are said to have a market share of over 90% in the Internet. They are used by most large

companies and agencies all over the world, and are considered as the most important building blocks of the Internet. Cisco routers provide physical connectivity between networks by virtue of their physical attachments to either local area networks (LANs) or wide area networks (WANs).

But, Cisco routers have several vulnerabilities that could allow hackers to disrupt Internet traffic, intercept sensitive information such as passwords and credit card numbers or redirect traffic from web sites. Securing the router is the first thing that network administrators need to do.

Therefore, for guarding both American national security and commercial security, it is really important to detecting, preventing and mitigating the DoS/DDoS attacks on the Cisco routers.

2. Three DoS/DDoS Attack Types to Cisco Routers

Denial of Service (DoS) attacks to Cisco routers are common on the Internet. The first step in responding to such an attack is to find out exactly what sort of attack it is. In general, there are three DoS/DDoS attack types.

2.1. Smurf

Smurf attacks are network amplification attacks, it is usually noticed because a network link becomes overloaded, so it is a network level attack. The attacker sends ICMP Echo Requests (pings) to the broadcast address of a network, so the victim is hit by many more packets. Smurf attacks cause each machine on the subnet to respond to the Echo Request with an Echo Reply. The attacker forges the source address of the ICMP Echo Request with the victim's IP address.

2.2. Fraggle

The Fraggle (UDP Packet Magnification) attack is the cousin of Smurf attack, Fraggle attack uses UDP echo packets in the same fashion as the ICMP echo packets. Fraggle usually achieves a smaller amplification factor than Smurf, so it is much less popular. On the other hand, the UDP echo is a less important service in most network than the ICMP echo, and can therefore be disabled completely with fewer negative consequences.

2.3. SYN flood

Another common attack is the SYN flood, in which a target machine is flooded with TCP connection requests. The source addresses and source TCP ports of the connection request packets are randomized; the purpose is to force the target host to maintain state information for many connections that will never be completed.

SYN flood attacks are usually noticed because the target host (frequently an HTTP or SMTP server) becomes extremely slow, crashes, or hangs. It's also possible for the traffic returned from the target host to cause trouble on routers; because this return traffic goes to the randomized source addresses of the original packets, it lacks the locality properties of "real" IP traffic, and may overflow route caches. On Cisco routers, this problem often manifests itself in the router running out of memory.

2.4. Summary

Together, the Smurf and SYN flood attacks account for the vast majority of the flooding DoS attacks reported to Cisco, and recognizing them quickly is very important.

A wide variety of DoS/DDoS attacks are possible, but many attacks are similar. Attackers choose common exploits because they are particularly effective, particularly hard to trace, or because tools are available. Many DoS/DDoS attackers lack the skill or motivation to create their own tools, and use programs found on the Internet; these tools tend to fall in and out of fashion.

Many of the commonly used DoS/DDoS attacks are based on high-bandwidth packet floods, or on other repetitive streams of packets. The packets in many DoS/DDoS attack streams can be isolated by matching them against Cisco IOS software access list entries. This is valuable for filtering out attacks, but is also useful for characterizing unknown attacks, and for tracing “spoofed” packet streams back to their real sources.

3. Four Programs to Launch Attacks

In general, the attackers use four programs (or tools) to launch DoS/DDoS attacks to Cisco routers:

3.1. Trinoo

It is a master/slave programs, Trinoo daemons were originally found in binary form on a number of Solaris 2.x systems, which were identified as having been compromised by exploitation of buffer overrun bugs in the RPC services “statd”, “cmsd” and “ttldbserverd”.

The Trinoo uses UDP for communication between handlers and agents.

Trinoo only initiates UDP attacks to random ports. Communication between master and slave is via unencrypted TCP and UDP. No IP spoofing. Uses following default ports to communication:

1524 TCP
17665 TCP
27444 UDP
31335 UDP

The Trinoo uses the ports listed above for orientation and example only, because the port numbers can easily be changed.

3.2. TFN (Tribal Flood Network)

It uses IP spoofing. Uses ICMP Echo reply packets to communicate between zombie and master (agent and handler).

One of the weaknesses of TFN was that the attacker’s connection to the master(s) that control the network was in clear-text form, and was subject to standard TCP attacks.

3.3. TFN 2K

Same as TFN – but the slave is silent so difficult to spot. No return information from the slave. Zombie to master communication is encrypted.

TFN 2K does not use any specific port (it may be supplied on run time or it will be chosen randomly by a program), but it is a combination of UDP, ICMP and TCP packets.

3.4. Stacheldraht

Stacheldraht (German for “barbed wire”) is a DDoS tool based on source code from the TFN, it combines features of the “Trinoo” DDoS tool, with those of the original TFN, and adds encryption of communication between the attacker and Stacheldraht masters and automated update of the agents. Stacheldraht uses TCP and ICMP for communication handlers and agents.

Stacheldraht uses following default ports to communication:

16660 TCP
 65000 TCP
 ICMP Echo
 ICMP Echo Reply

The Stacheldraht uses the ports listed above for orientation and example only, because the port numbers can easily be changed.

Remote control of a Stacheldraht network is accomplished using a simple client that uses symmetric key encryption for communication between itself and the handler. The client accepts a single argument, the address of the handler to which it should connect. It then connects using a TCP port (default 16660 tcp in the analyzed code).

4. Controlling Directed Broadcasts -- Against the DoS/DDoS Attacks (Smurf)

IP directed broadcasts are used in the Smurf Denial of Service (DoS) attacks, and can also be used in related attacks.

An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. The directed broadcasts are occasionally used for legitimate purposes, but such use is not common.

The Smurf attacks send ICMP echo requests from a spoofed source address to a directed broadcast that cause all hosts to respond to the ping echo request, creating a lot of traffic on the network. So by default on IOS version 12.0 and higher, command “ip directed broadcast” is disabled; if you are running any version lower than 12.0, the command should be applied to every LAN interface that isn’t known to forward legitimate directed broadcasts. It is imperative that you disable IP directed broadcasts on the router by issuing the following command in interface configuration mode:

```
Router(config-if)#no ip directed-broadcast
```

If a Cisco interface is configured with the no ip directed-broadcast command, directed broadcast that would otherwise be “exploded” into link-layer broadcasts at that interface are dropped instead. Note that this means that no ip directed-broadcast must be configured on every interface of every router that might be connected to a target subnet; it is not sufficient to configure only firewall routers.

5. Tracing

If you setup the access list as follows:

```
access-list 169 permit udp any any eq echo  

access-list 169 permit udp any eq echo any  

access-list 169 permit icmp any any echo  

access-list 169 permit icmp any any echo-reply  

access-list 169 permit tcp any any established  

access-list 169 permit tcp any any
```

Then this list doesn’t filter out any traffic, all the entries are permits. However, the list categorizes

packets in useful ways, the list can be used to tentatively diagnose all three types of attacks: Smurf, Fraggle and SYN Floods.

5.1 Tracing with “log-input”

If you choose to trace an attack passing through a Cisco router, the most effective way of doing so is to construct an access list entry that matches the attack traffic, attach the log-input keyword to it, and apply the access list outbound on the interface through which the attack stream is being sent toward its ultimate target. The log entries produced by the access list will identify the router interface through which the traffic is arriving, and, if the interface is a multipoint connection, will give the Layer 2 address of the device from which it is being received. The Layer 2 address can then be used to identify the next router in the chain, for example, the show ip arp mac-address command.

5.2 Tracing SYN Flood

To trace a SYN flood, you might create an access list similar to the following:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

This will log all SYN packets destined for the target host, including legitimate SYNs. To identify the most likely actual path toward the attacker, examine the log entries in detail. In general, the source of the flood will be the source from which the largest number of matching packets are arriving. Remember that the source IP addresses themselves mean nothing; you are looking for source interfaces and source MAC addresses. Sometimes it is possible to distinguish flood packets from legitimate packets because flood packets may have invalid source addresses; any packet whose source address is not valid is likely to be part of the flood.

Remember that the flood may be coming from multiple sources, although this is relatively unusual for SYN floods.

5.3 Tracing Smurf

To trace Smurf stimulus stream, use an access list like this:

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

The first entry doesn't restrict itself to packets destined for the reflector (the second victim) address. The reason for this is that most Smurf attacks use multiple reflector networks. If you are not in contact with the ultimate target, you may not know all the reflector addresses. As your trace gets closer to the source of the attack, you may begin to see echo requests going to more and more destinations; this is a good sign.

However, if you are dealing with a great deal of ICMP traffic, this may generate too much logging information for you to read. If this happen, you can restrict the destination address to be one of the reflectors that's known to be used. Another useful tactic is to use an entry that takes advantage of the fact that netmasks of 255.255.255.0 are very common in the Internet. And because of the way that attackers find the Smurf reflectors, the reflector addresses actually used for Smurf attacks are even more likely to match that mask. Host addresses ending in .0 or .255 are very uncommon in the Internet, so you can build a relatively specific recognizer for Smurf stimulus streams like this:

```
access-list 169 permit icmp any host known-reflector echo log-input
```

```
access-list 169 permit icmp any 0.0.0.255 255.255.255.0 echo log-input
access-list 169 permit icmp any 0.0.0.0 255.255.255.0 echo log-input
access-list 169 permit ip any any
```

With this list, you can eliminate many of the “noise” packets from your log, while still having a good chance of noticing additional stimulus streams as you get closer to the attacker.

5.4 Tracing without “log-input”

The log-input keyword exists in Cisco IOS Software Releases 11.2 or later. Older software does not support this keyword. If you are using a router with older software, you have three viable options:

1. Create an access list without logging, but with entries that match the suspect traffic. Apply the list on the input side of each router interface, and watch the counters. Look for interfaces with high match rates. This method has a very small performance overhead, and is good for identifying source interfaces. But it has a biggest drawback: it doesn't give the link-layer source addresses, so it is only useful mostly for point-to-point lines.
2. Create access list entries with the log keyword. Apply the list to the incoming side of each interface of a router. This method still doesn't give source MAC addresses, but can be useful for seeing IP data, for instance to verify that a packet stream really is part of an attack. Performance impact can be moderate to high; newer software performs better than older software.
3. Use debug ip packet detail command to collect information about packets. This method gives MAC addresses, but it can have serious performance impact. It's easy to make a mistake with this method and make a router unusable. If you use this method, make sure that the router is switching the attack traffic in fast, autonomous, or optimum mode. Use an access list to restrict debugging to only the information you really need. Log debugging information to the local log buffer, but turn off logging of debug information to Telnet sessions and to the console. If possible, arrange for someone to be physically near the router, so that it can be power cycled as necessary.

6. References

Cisco – Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks:

<http://www.cisco.com/warp/public/707/newsflash.html>

Magnification Attacks: Smurf, Fraggle, and Other:

<http://pintday.org/whitepapers/dos-smurf.shtml>

Cisco – Characterizing and Tracing Packet Floods Using Cisco Routers:

<http://www.cisco.com/warp/public/707/22.html>

Improving Security on Cisco Router:

<http://www.cisco.com/warp/public/707/21.html>

<http://security.uchicago.edu/seminars/DDoS/smurf.shtml>

Network Security Library: *Cisco Router Security Overview*

<http://www.secinf.net/info/fw/cisco/cisco.html>

Securing Cisco Routers: Author: Joshua L. Wright, John N. Stewart; Publisher: SANS Institute; Issue: November 1, 2002; ISBN: 0972427333.

About the Author

Hang Chau

Senior Network/System Administrator, Ming Plaza Development

hcdanny@yahoo.com

(909)864-9456

28925 Clear Spring Lane, Highland, CA 92346, U.S.A.

Degree and IT Certifications:

M.S. on Computer Science, California State University, Fresno, California, USA;

- CCIE, CCNP, CCNA (Cisco/CCIE: passed the Qualification Exam);
- SCSA, SCNA (Sun/Solaris 8: Certified System and Network Administrators);
- SCJP, SCWCD (Sun/Java 2: Certified Programmer and Web Component Developer);
- MCSE, MCSA (Microsoft 2000 Certified System Engineer and System Administrator).

Also research on Network Attacks and Network Security:

- Cisco IDS/Secure PIX (Intrusion Detection Systems and Firewall);
- DoS/DDoS (Denial of Service/Distributed Denial of Service);
- Mydoom/Doomjuice Worms and DoS/DDoS attacks.