Reflective DDoS Protection 101

Seth Garrett (sbgarret@iu.edu)
Network Engineer, Indiana University

Overview

The purpose of this guide is to help organizations start defending their networks from some of the more common Distributed Denial of Service (DDoS) attacks. Many reflective attacks utilize services that can be safely blocked or rate limited using existing hardware. These types of attacks utilize vulnerable services on hosts to redirect an amplified response back to a spoofed IP which ends up being the victim's IP. Reflective DDoS attacks are some of the most common due to how easy they are to launch.

This is not an all-inclusive guide to stopping all DDoS attacks. However, enhancing your understanding of these more common reflective DDoS attacks will help prepare you to have a better understanding of how to deal with some of the more complex attacks.

Traffic Analysis

Before even attempting to mitigate DDoS attacks, it is important that you have the ability to analyze your network traffic. Having a solid understanding of the existing traffic patterns on your network will be critical in identifying abnormal traffic patterns. Your ability to block or rate limit certain traffic patterns is going to be unique to your organization. Software that can analyze sampled flow data from your routers is recommended. The following items some items you should look for in a traffic analyzer:

- Source & Destination IP
- Source & Destination Port
- Average Packet Size
- Protocols
- If sampling traffic, the software should allow you to add a sampling multiplier.
- Alerting mechanisms based upon traffic patterns or thresholds.

Be cautious when sampling traffic 1:1. Often times this itself can lead to a DDoS attack having a negative impact on your network due to overwhelming your router platform. 1:100 and 1:1000 are more commonly seen flow sampling ratios.

Internet Service Provider (ISP) Involvement

Engaging your ISP is another important piece to DDoS protection. Many of the blocks and rate limits you will want to perform are better served being done on the ISP side of the network paths. Ultimately this helps save your internet link itself from being a victim of such attacks. For example, during a 50Gbps NTP based reflective attack, it is a lot less effective to start blocking it once it has already shown up on your organization's network. You may find that your ISP already has some protection mechanisms or services available. Its best to address these items proactively so that you know what is available for planning or in response to a crisis. Items to address with your ISP:

- Do you have a Remotely Triggered Black Hole (RTBH) solution that we can use?
- Can we specify ports and protocols that we want either blocked or rate limited on your router interface(s) facing our network?
- Do you provide any DDoS protection services we can take advantage of?

Reflect DDoS Attack Types & Recommendations

Below is a list of some of the more common reflective DDoS attacks. This should serve as a guide to point you towards some areas to look at along with a recommendation. You should consult your organization's existing traffic patterns before actually taking action based on any of these recommendations. These recommendations are based off performing changes on your internet path for traffic destined towards your network. You should not blindly make any changes based off this without a thorough evaluation of your existing traffic patterns.

- **NTP (UDP 123)**
    - Recommendation: Rate limit NTP over 128 bytes. Most reflective DDoS attacks using NTP will be made up of datagrams of 400 bytes or more. Legitimate NTP traffic often falls under 128 bytes.
- **SSDP (UDP 1900)**
    - Recommendation: Block by default. If you cannot block, then rate limit it.
- **RIPv1 (UDP 520)**
    - Recommendation: Block by default. If you cannot block, then rate limit it.
- **NETBIOS (UDP 137)**
    - Recommendation: Block by default. If you cannot block, then rate limit it.
- **SNMP (UDP 161)**
    - Recommendation: Block by default. If you cannot block, then rate limit it. You should also analyze your existing traffic patterns to identify and make exceptions for any legitimate SNMP traffic.
- **CHARGEN (UDP 19)**
    - Recommendation: Block by default.
- **RPC Portmapper (UDP 111)**
    - Recommendation: Block by default.
- **DNS (UDP 53) & IP Fragments**
    - Recommendation: Identify and make exceptions for legitimate DNS traffic to servers on your network. Rate limit all other DNS traffic.

    - Reflective DDoS attacks using DNS will also be made up of IP fragments. These fragments will be a large portion of the attack. You evaluate both your DNS and fragment traffic patterns to determine the proper levels to rate limit them on.
    - Its best to utilize a method that is made up of multiple rate limiters for DNS attack traffic. Putting all of your DNS traffic through one policer can be problematic.
    - Flow analyzers often times report fragments as UDP port 0.
- **Odd UDP Port Combinations**
    - Another avenue to blocking reflective DDoS attack traffic is to target specific port combinations. For example, blocking UDP datagrams with source port 123 and destination port 53 is pretty safe. Often times attackers will use a reflective attack to target specific service ports on your network. In this case, they would be trying to attack port 53 using an NTP reflective DDoS attack.

Rate Limiting Caution

You should always take caution when rate limiting traffic. When not done properly, it can create problems just as bad as the DDoS attack or worse. Juniper routers have a firewall filter/ACL action called prefix-action that can be utilized to assist with this problem. When using functionality like this, you can take traffic matching a single ACL term and police it across thousands of rate limiters depending on the destination IP address. The benefit is that when the rate limit is hit, it will only start dropping traffic for that destination IP and a smaller group of other IPs sharing the same rate limiter. Cisco has a similar type of feature called Microflow Policing. You should consult your hardware platform to see if similar capabilities are available to help dilute an attack in this manner.

Conclusion

I think it is safe to say at this point that DDoS attacks should have a spot at the table when designing and supporting computer networks at just about any organization. I hope this helps raise awareness around some common reflective DDoS attack types along with some potential ways to proactively stop them. There are many attack methods not covered in this document, but hopefully this helps serve as a starting point in getting involved in DDoS protection.