Neustar® Insights

Four Tools to Capture DDoS Attacks in Monitoring

neustar®
Real Intelligence. Better Decisions.™

Most cloud DDoS mitigation services are offered on-demand, meaning that customers can enable the service when they are the victim of a DDoS attack. But how can a company find out – quickly – that it is under attack? Sometimes it is difficult to know.

Below are four monitoring tools to help companies identify and protect against DDoS attacks.

Option #1 – Internal Server, Network and Infrastructure Monitoring Applications

Companies have a lot of monitoring software and applications to choose from, but one of the more popular pieces of software, called Nagios, allows you to monitor internal infrastructure status and performance of applications, services, operating systems, network protocols, system metrics and network infrastructure.

For example, monitoring software can check your HTTP service to ensure that a Website or Web server is functioning properly, and if the service is not functioning, most software includes real-time notification. Because most DDoS attacks target a Web server or application server, monitoring software may show the HTTP service to be experiencing a problem with slowness, high memory/CPU utilization or complete failure. In these situations, something is obviously wrong and it could be a DDoS attack.

While monitoring servers and infrastructure are helpful, there is no guarantee that DDoS is the culprit. Abnormal spikes in traffic and usage do occur for legitimate reasons.

It's up to the IT administrator to then assess the data and determine whether to enable a DDoS mitigation service.

Option #2 – External Performance Monitoring Solutions in the Cloud

A second approach IT administrators can use to assess a potential DDoS attack is to use an external performance monitoring solution. Unlike network/infrastructure tools — which are usually installed inside a customer's network — external performance monitoring solutions are typically provided by a third party and leverage monitoring locations from around the world.

External monitoring tools can encompass several elements:

1. Virtual browsers to check for basic Website / application uptime and performance
2. Real browsers to check for Website / application performance, errors and service degradation
3. Network services such as DNS, FTP and email, among others

From a DDoS perspective, an external third-party monitoring solution makes sense. The purpose of this type of solution is to constantly monitor a Website, service or application and notify the user of downtime, slow responses or other issues. All of these are potential indicators of a DDoS attack.

That said, although a third party external monitoring solution can work at capturing DDoS attacks, these solutions are not foolproof. An external solution can tell an IT administrator that performance is degrading or has failed, but it cannot determine the reason.

Originally, the goal of third-party monitoring was to ensure that ISPs, hosting companies and servers were functioning as designed. Slow response times and outages could indicate a provider or server being down.

As mentioned in option one of this series, it is important to carefully analyze any data from a third-party before enabling your DDoS protection service.

Companies that do not host their own Websites and use third parties like Amazon EC2 would benefit the most from third-party monitoring solutions.

Option #3 – Netflow / Peakflow Traffic Analysis & Monitoring

Monitoring Netflow data is another good option for detecting DDoS. Netflow, a protocol designed by Cisco Systems for collecting IP traffic information, has become a standard in the industry, and it is widely used and supported on multiple platforms.

Cisco defines Netflow data as a sequence of packages that include the following values:

1. Ingress interface
2. Source IP address
3. Destination IP address
4. IP protocol
5. Source port for UDP / TCP, 0 for other protocols
6. Destination port for UDP / TCP, type and code for ICMP, or 0 for other protocols
7. IP type of service

Some DDoS mitigation providers can take samples of your Netflow data and proactively notify you of possible attacks. For example, a DDoS mitigation provider will analyze network data for a period of time and define normal baseline activity. Once a baseline is established, abnormally high and low thresholds can be set for various factors, such as bandwidth utilization, packets per second or protocol misuse.

The provider will establish low, medium and high thresholds for alerting purposes. When a threshold is exceeded, the provider will notify you by email, phone or some other agreed upon method. As always, you would want to evaluate the data before enabling mitigation.

Some businesses—for example, those using third-party hosting solutions—are unable to export Netflow data, because it generally requires you to own or lease your own routers. In such cases, third-party external monitoring solutions are an option.

Option #4 – On Premise DDoS Equipment (with Cloud DDoS Mitigation Backup)

The final option for capturing DDoS in monitoring involves installing an on-premise DDoS device in your network or data center. Unlike previous options, an on-premise DDoS device will actually perform mitigations, handling attack traffic as it passes through the device.

Some cloud DDoS mitigation services provide a managed solution, a hybrid of on-premise equipment and cloud protection as a backup. The on-premise device will handle any DDoS attacks up to the size of the available bandwidth. If an attack exceeds the bandwidth, the cloud service can be turned on.

While an on-premise device would seem to be the most attractive solution, compared to the other monitoring options we've discussed, it will also likely be the most expensive. Additionally, you cannot implement it in shared hosting or cloud computing environments like Amazon EC2.

Conclusion

DDoS attacks are a growing problem, and companies have been scrambling to put cloud protection in place. The question for them now is "How do we know if we are under attack?"

Each of the options we've covered has its pros and cons. You need to evaluate your infrastructure, budget and any concerns you may have about specific options in order to find the best solution for your business.

While no solution is perfect, "Hope for the best, prepare for the worst" is a good mantra.

About Neustar

Neustar, Inc. (NYSE: NSR) is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, information services, financial services, retail, media and advertising sectors. Neustar applies its advanced, secure technologies in location, identification, and evaluation to help its customers promote and protect their businesses. More information is available at **www.neustar.biz.**

21575 Ridgetop Circle, Sterling, VA 20166
+1 571.434.5400 / www.neustar.biz

ES-WP-DDos-017-4 ways-tools-capture-ddos-attacks-v020414

neustar®
Real **Intelligence.** Better **Decisions.**™