How to block HTTP DDoS Attack with Cisco ASA Firewall

Denial of Service attacks (DoS) are very common these days. Especially Distributed DoS attacks (called also DDoS) can be executed quite easily by attackers who own large networks of BotNets. Thousands of malware-infected computers (which comprise the so called “BotNets”) are controlled by attackers and can be instructed to start attacks at any target.

Usually WebSites are targeted more frequently. Bringing down a website can have a negative effect to the image (in addition to any financial loss) of the company owing the site. A DDoS attack can be purely “volumetric”, which means that the attacker just sends high volume of packets as quickly as possible to flood the bandwidth of the “pipe” connecting the website to the Internet. Also, DDoS attacks can be “Application Resource Exhaustion” which means that the attacking computers create thousands of application requests (e.g HTTP Requests) to a server, thus consuming the application resources.

A Cisco ASA Firewall can not help much in a “volumetric” DDoS attack. In such an attack, a dedicated DDoS device is needed or your ISP must do some kind of rate limiting to mitigate the attack. However, for “Application Exhaustion” attacks a Cisco ASA can help to some extend with HTTP inspection using the Modular Policy Framework mechanism of ASA. This is what we are going to describe in this article.
Usually, HTTP Application DDoS attacks have a pattern or string which helps you distinguish the attacking HTTP requests from other legitimate requests. For example, HTTP attacking packets might have a common parameter or string, which can be for example the same “User-Agent” used by the attacking script, a common POST or GET URI request, some other HTTP header parameters etc. With the ASA HTTP inspection feature you can match on this common pattern in the HTTP packet thus filter-out the attacking packets and drop them.

Recently I was engaged to help mitigate a DDoS attack on a webserver. I observed from the Apache logs that the attacking HTTP requests were all targeting the website on the same URL string, such as http://www.website.com/xyz123. The string “xyz123” was the common pattern for all malicious HTTP requests. Thus with a policy on ASA you can match on the unique string above and drop the packets that have this string in the HTTP URI.

Let's see a diagram and configuration below:
ASA Configuration:

!First create a regular expression with the unique attack string
regex attackstring xyz123

!Create an ACL to match the HTTP traffic towards the target server
access-list HTTPTRAFFIC extended permit tcp any host 1.1.1.1 eq www

!Create a regular L3/L4 class to match the traffic above
class-map attackingtraffic
  match access-list HTTPTRAFFIC

!Now create an HTTP inspection policy to match on the unique attacking string
policy-map type inspect http HTTPDOS
  parameters
  match request uri regex attackstring
    drop-connection
  match request args regex attackstring
    drop-connection
!The following policy-map will include the L3/L4 class which will include the HTTP inspection policy

```
policy-map BLOCKDOS
  class attackingtraffic
    inspect http HTTPDOS
```

!Now attach the policy-map to the ASA outside interface to inspect Inbound traffic.

```
service-policy BLOCKDOS interface outside
```

If you enable logging on the drop-connection command (use “drop-connection log”), then you will start seeing logs that the ASA is dropping packets with the matched attacking HTTP string.

---

**About the Author**

Harris Andrea is a Cisco Certified Professional with more than 18 years of experience working with Cisco network technologies. He is the author of two Cisco Books (“Cisco ASA Firewall Fundamentals” and “Cisco VPN Configuration Guide”) which have been embraced by thousands of Cisco professionals all over the world. You can find more Cisco configuration guides and tutorials on his blogs below:

- [http://www.networkstraining.com](http://www.networkstraining.com)
- [http://www.tech21century.com](http://www.tech21century.com)