EtherealMind.com
Being Human Infrastructure & My Life in IT

You are here: Home / Design / TCP SYN Cookies – DDoS defence

TCP SYN Cookies – DDoS defence

12TH SEPTEMBER 2008 BY GREG FERRO
FILED UNDER: DESIGN, SECURITY

A TCP SYN Cookie is typically used in DDoS engines and load balancers to create another level of protocol security for Denial of Service attacks. Lets take a quick dive through the technology.

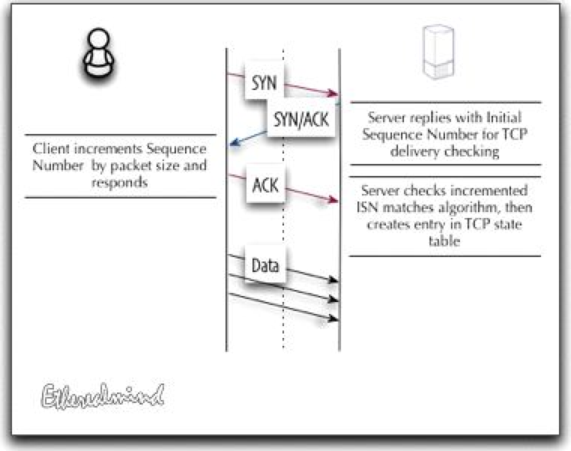
What is a SYN Cookie and Why do I want them ?

A SYN cookie is a specific choice of initial TCP sequence number by TCP software and is used as a defence against SYN Flood attacks.

In normal operation, a Client sends a SYN and the Server responds with a SYN+ACK message, the server will then hold state information in the TCP stack while waiting for Client ACK message. A simple SYN flood (using suitable software) will generate SYN packets which would consume all available TCP memory as the server must maintain state for all half-open connections. And since this state table is finite the server will no longer accept new TCP connections and thus fail or *deny service* to the user ([or worse, buffer overflows or system memory exhaustion has occurred, not so much a problem today]).

This is highly leveraged attack since a very small amount of bandwidth and CPU can exhaust the resources on a large number of servers.

By specifically calculating the TCP sequence number with a specific, secret math function in the SYN-ACK response, the server does not need to maintain this state table. On receipt of the ACK from the Client, the TCP sequence number is checked against the function to determine if this is a legitimate reply. If the check is successful, then the server will create the TCP session and the user connection will proceed as normal.


SYN
SYN/ACK
Server replies with Initial Sequence Number for TCP delivery checking
Client increments Sequence Number by packet size and responds
ACK
Server checks incremented ISN matches algorithm, then creates entry in TCP state table
Data
Etherealmind

The TCP sequence number at the commencement of a TCP sequence is normally a randomised choice. The TCP sequence is what NMAP uses to identify the OS since it 'knows' the some OS's do not have high quality randomisation and NMAP uses algorithms to analyse the ISN to 'guess' the OS. This is part of the functions of a PIX/ASA firewall, it will improve the randomness of the ISN to ensure

If the ACK response is not correct the TCP session is not created. The effect is that SYN floods will no longer consume resources on servers or load balancers/ This is especially true in high bandwidth environments such as Data Centres.

How should I implement SYN Cookies ?

In general terms, implementing this type of code on servers is a bad idea. The CPU requirement to deliver the mathematics for the function calculation is beyond the capacity of x86 servers (and their OS's) to reliably compute on a real time basis ((although a MSWin / Linux server certainly could compute the functions, its overall performance would be severely impacted)). The CPU impact may result in servers not able to deliver applications or, at best, to work much more slowly in every circumstance.

The most common implementation is on load balancer and DDoS appliances, with dedicated CPU and OS that can process huge volumes of TCP sequence calculations without loss of performance. In this case, the TCP establishment is handled by using session termination or by session interception.

DDoS engines ((why are they called engines instead of appliances ? I don't know, thats what I call them. Must be a marketing thing)) will also use SYN cookies e.g. The Cisco Guard will use SYN cookies as a first level of DDoS defence once traffic is diverted to the module.

Should you be implementing ?

SYN Cookies is a simple DDoS defence today, and probably suitable for all Internet hosting including mail server and corporate web servers.

Many DDoS attacks will simply overrun your Internet connections with volume since a 100 MB ethernet connection is now very small compared to, for example, 500 compromised desktops with an average 200 Kbs of bandwidth each launching an attack will saturate your 100Mbs link and there is nothing you can do ((at this point you will need to use your service provider to mitigate the attack)). But a SYN attack can be accomplished with a 2Mbs DSL line and is unlikely to overrun your bandwidth (since a SYN packet is 64 bytes).

Alternatives to SYN Cookies

You don't have to use SYN cookies to defend against a SYN flood because most modern firewalls will monitor the state table, and discard connections once a high water mark has been reached. Of course, smarter firewalls will look at SYN packets per second per protocol and start to flag an attack plus start to purge half open connections to ensure resource availability. But they often do not have intelligent routines and may actually discard good TCP sessions, especially with high volume attacks) and thus cause a degraded service while the attack continues.

Conclusion

I have to admit that Internet DDoS attacks is something of a specialist art, and practitioners must stay up to date with current trends. Experience is vital, not only in using the equipment, but in recognition and identifying new attacks. I am not one of them.

TCP SYN cookies is useful tool for preparing a defence in medium sized networks where spending money on a managed DDoS service is not possible.

Feedback

You leave a comment below, or head over to the forums at http://etherealmind.com/forums and start a topic. Look forward to hearing from you.

Reference

DJ Bernstein has an excellent post here which includes a lot of history and it's early development sometime around 1997.

The Wikipedia is also a good source of information here

A very complete definition Defenses Against TCP SYN Flooding Attacks, warning this is a deep technical paper – geek meter pegs at eleven. [Thanks to Netfortius on twitter]

About Greg Ferro
Greg is surprisingly passionate & committed to treating people as humans that are profit-generating productivity tools instead of 'fleshy IT robots as a cost centre'. Survived 25 years of Corporate IT across

many verticals and tens of companies working on a wide range of networking solutions & products.
Host of the Packet Pushers Podcast on data networking at https://packetpushers.net- now the largest networking podcast on the Internet.
My personal blog at https://gregferro.com

COMMENTS

Arturo Servin says
12th September 2008 at 12:43 +0100

Excellent post and very good references. I am doing my research on DoS and DDoS and this will be very helpful.

Thanks,
-as

Thomas Jones says
10th February 2010 at 01:59 +0100

What's this about syn cookies being too computationally expensive? That's just rubbish

Thomas Jones says
10th February 2010 at 02:02 +0100

see here:

http://lwn.net/Articles/277146/

Syncookies take a system from serving nothing (due to syn flood) to almost as much as it does under no flood.

Also syn cookies impose no extra cost unless the system is actually under attack or very heavy load (ie it would have just dropped the connection)

Greg Ferro says
10th February 2010 at 07:20 +0100

The loads they discuss here aren't really significant. Typically, I'm designing for archictectures that have around 500K to 1 million concurrent HTTP session. Syn cookies are not implemented on the servers since the code complexity reduces system reliability and are handled at the network layer. Also, Linux sysadmins don't typically have networking skills that comprehend TCP SYN floods.

That said, it's usually the network person securing against a SYN Flood and not the server team. Therefore handling SYN floods at the network is far more common. YMMV.

Note: At loads of 1 million concurrent sessions, you wouldn't be using an IOS router but dedicated device.

Webscopia says
17th August 2010 at 21:17 +0100

Does FreeBSD with PF enabled – is that able to totally block Syn Attacks by proxying them 100%?

NETWORK BREAK PODCAST

Network Break is round table podcast on news, views and industry events. Join Ethan, Drew and myself as we talk about what happened this week in networking. In the time it takes to have a coffee.

PACKET PUSHERS WEEKLY

A podcast on Data Networking where we talk nerdy about technology, recent events, conduct interviews and more. We look at technology, the industry and our daily work lives every week.

Our motto: Too Much Networking Would Never Be Enough!

FIND ME ON SOCIAL MEDIA

Return to top of page

Opinions, Views and Ideas expressed here are my own and do not represent any employer, vendor or sponsor.Full disclosure