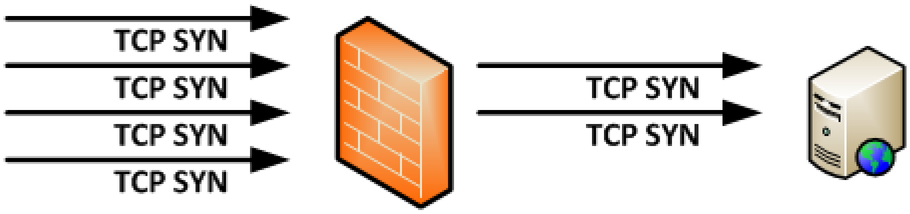
TYPES OF DOS ATTACK

Everyone has heard of a DoS attack: a Denial of Service attack that consumes a server's resources, taking it (temporarily) offline. However, more that one type of DoS attack exists. I'm going to discuss a few here to clarify the complexity in defending against them.

The SYN attack



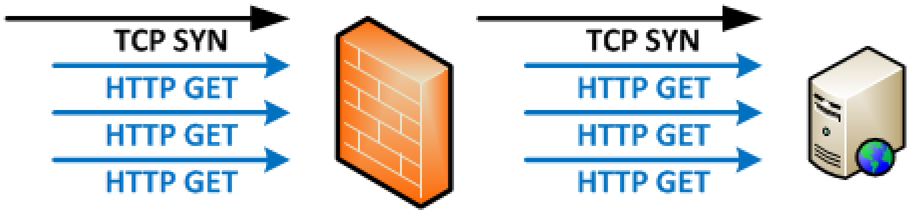
One of the most simple and well-known DoS attacks: just sent TCP packets with only the SYN flag set towards a web server. The server will reserve resources (sockets, memory, CPU) for the incoming connections and reply, but the connection is never completed. This can go up to millions of packets per second.

While this will take down a server eventually, it can also affect the firewall in front of it: the state table will fill up. Worst case this affects reachability of all servers behind the firewall.

One way to deal with this is rate-limiting the number of incoming connections towards each server on the firewall if the firewall supports it, making it one of the few attacks that can be countered without a dedicated anti-DoS appliance.

Another way is using SYN cookies: the firewall will send the reply (SYN,ACK) on behalf of the server and only if the client completes the connection (ACK), the firewall will connect to the server and tie both connections together.

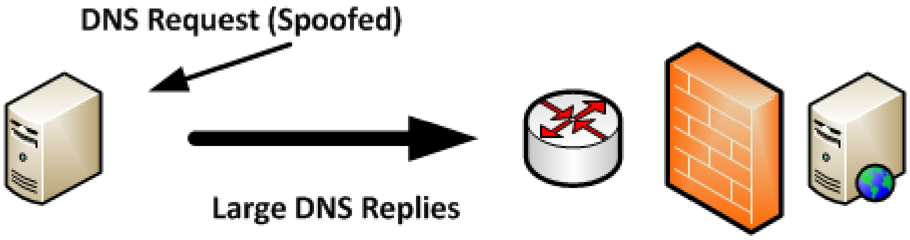
The HTTP GET attack



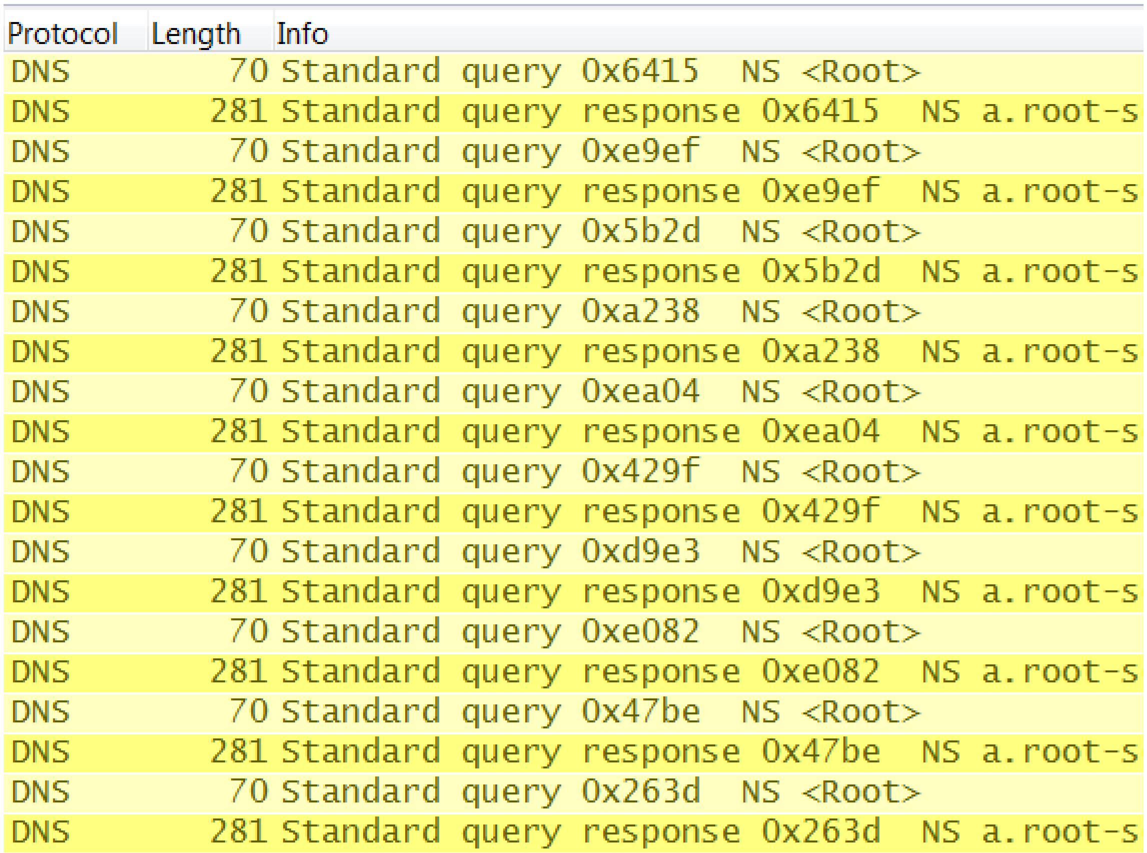
This attack bypasses the firewall, making it much more difficult to counter. A single TCP connection towards a web server is established. In that connection, instead of requesting the web page once using an HTTP GET, the web page is continuously requested over and over again, using up all server resources.

Countering this requires packet inspection on layer 6-7 which must be done by an IPS or anti-DoS appliance. Firewalls will not detect this.

The UDP flooding attack



A UDP flooding attack is most often done using open DNS resolvers. A DNS request with a spoofed source IP address is sent towards a DNS server. This DNS server replies towards the spoofed IP address (the target server) with a large output. An example is a NS query for the root servers: the response is about four times larger compared to the request. This means about 250 Mbps of request traffic is required to flood a gigabit uplink towards a server in this case.



Protocol	Length	Info
DNS	70	Standard query 0x6415 NS <Root>
DNS	281	Standard query response 0x6415 NS a.root-s
DNS	70	Standard query 0xe9ef NS <Root>
DNS	281	Standard query response 0xe9ef NS a.root-s
DNS	70	Standard query 0x5b2d NS <Root>
DNS	281	Standard query response 0x5b2d NS a.root-s
DNS	70	Standard query 0xa238 NS <Root>
DNS	281	Standard query response 0xa238 NS a.root-s
DNS	70	Standard query 0xea04 NS <Root>
DNS	281	Standard query response 0xea04 NS a.root-s
DNS	70	Standard query 0x429f NS <Root>
DNS	281	Standard query response 0x429f NS a.root-s
DNS	70	Standard query 0xd9e3 NS <Root>
DNS	281	Standard query response 0xd9e3 NS a.root-s
DNS	70	Standard query 0xe082 NS <Root>
DNS	281	Standard query response 0xe082 NS a.root-s
DNS	70	Standard query 0x47be NS <Root>
DNS	281	Standard query response 0x47be NS a.root-s
DNS	70	Standard query 0x263d NS <Root>
DNS	281	Standard query response 0x263d NS a.root-s

Larger multipliers exist for other types of queries, generating 10, 20, 30,… times as much output compared to the query. While this example uses DNS, UDP-based attacks now also exist for NTP and SNMP. Advantages of NTP and SNMP are large possible multiplier values and less awareness of the attack’s existence.

However, the bad part is that this kind of attack floods uplinks towards data centers and LANs, which are shared with other servers or companies. Placing an anti-DoS appliance in the data center right before the firewall, but after the uplink towards the ISP, will be ineffective. Countering this attack requires an appliance at the ISP before the uplink, or DoS cloud services that reroute BGP IP ranges (assuming you have them) for filtering in case of a large-scale DoS.

Without an appliance options are limited. Placing a firewall in front of it will demand a lot of CPU from the firewall as it will still have to receive, check and drop packets. Usually two options remain: switch ACLs and black hole routing. Black hole routing means setting up a Null route of the destination server before it reaches your infrastructure (an ISP or BGP router), essentially giving up your server to save the rest of the network. ACLs on switches are hard to set up in the middle of an attack and not always possible, but the advantage is that packets will be dropped in hardware, using the switch ASIC and not consume any firewall, router or server CPU. Most likely your server will still end up unreachable.

Others

The above are just a few common ones. Fact is, any layer 3 point in the network can be attacked. Even if it doesn't have any ports listening, it will have to use CPU to look at packets arriving for the IP address it has. And if it's a web server behind a firewall, it will be reachable on a port which can be exploited. Encryption (SSL) can ironically make this worse because anti-DoS appliances can't check in the HTTPS session for GET requests, or the encryption itself can be continuously renegotiated, taking up CPU.

Remember, most DoS attacks are legitimate packets. Just a lot of them.

Source : http://reggle.wordpress.com/2014/02/07/dos-attack-types/