Best Practice - How to Protect Against DoS Attacks

https://campus.barracuda.com/doc/73718976/

The following article explains how to use the Barracuda CloudGen Firewall to protect against DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks. Various attack mitigation mechanisms integrated into the Barracuda CloudGen Firewall engine enable you to do this.

TCP SYN Flooding Protection

The Barracuda CloudGen Firewall offers a choice of two different connection request acceptance policies on a per-rule basis that are intended to offer varying levels of protection against TCP SYN flooding attacks.

- **Outbound Accept Policy** – "Trusted clients accessing untrusted networks": When outbound behavior is selected, TCP sessions are established between the two communicating network entities. The firewall system merely analyses the datagrams passively and keeps an internal state table of the TCP session.
- **Inbound Accept Policy** – "Server protection against untrusted networks": For inbound behavior, a TCP session is first established between the initiating source and the Barracuda CloudGen Firewall before any information flow is forwarded to the desired destination. Only after a TCP session between the initiator and the firewall system has been established does the firewall actively generatesTCP datagrams in order to establish a TCP session with the destination.

For information on how to configure TCP Syn Flooding Protection, see: Best Practice - Protect Against TCP SYN Flooding Attacks with TCP Accept Policies.

TCP SYN Cookies

Upon successful establishment, the TCP session is governed directly by the two communicating network entities. In order to protect itself from resource exhaustion due to a large number of information flow requests being created in short succession, the firewall can switch to an alternative mode in which TCP information flow request information is no longer stored in memory but rather coded into the sequence number used for TCP session initiation. These sequence numbers are called SYN-COOKIES and allow the firewall to check whether a received datagram is a response to a datagram previously generated on the firewall system.

For information on how to configure the settings for SYN cookie usage, see: General Firewall Configuration.

Duplicate Local IP Detection

Problems on the network are caused when IP addresses assigned to the firewall appear on another system within the same collision domain. Since another system in the network is now ARP battling the firewall for IP traffic, the data flow across the firewall is severely impaired. The firewall will check for such duplicate IP addresses and immediately alert the administrator through event messages.

For information on how to configure the eventing settings, see: Events.

Resource Exhaustion Protection

IP spoofing protection via the REP check and TCP SYN flooding protection already provide basic protection against naive DoS attacks. However, more sophisticated DoS attacks go beyond SYN flooding and typically involve connectionless protocols, such as UDP or ICMP, and usually occur from the Internet where the REP check will not help. The Barracuda CloudGen Firewall allows you to configure two resource limits on a per-rule basis to protect against resource exhaustion of the firewall gateway. The first limit is an overall limit for all sessions handled by the respective rule; the second one limits the maximum number of sessions per source address handled by the respective rule.

For connectionless protocols (UDP, ICMP-Echo, and all others except TCP), the firewall must create so-called pseudo-sessions. Using, for example, DNS requests, an attacker can create a massive amount of UDP pseudo-sessions within a short time period. For this reason, the gateway has configurable thresholds for the overall and per-source maximum number of allowed pseudo-sessions for the protocols UDP, ICMP-Echo, and all other IP protocols except TCP. For both operational and security reasons, each service (IP protocol and port if applicable) has configurable timeouts after which an idle session is terminated. For connectionless protocols, a so-called balanced timeout is also configurable. It determines the maximum allowed idle time before a session is closed in case a reply is received from the destination system. This balanced timeout is usually chosen much shorter than the actual timeout to warrant quicker dismantling of pseudo-sessions.

For information on how to configure forwarding limits, see: Forwarding Firewall Settings.

Firewall Session Monitoring

Although all the mechanisms mentioned in the previous section can protect the firewall (and servers protected by it) from resource exhaustion, they are ineffective against attacks aimed at bandwidth exhaustion. In a massive DDoS attack, the attackers may simply aim at saturating the link by transmitting vast numbers of UDP packets. The integrated environmental Monitoring and Reporting

feature of the Barracuda CloudGen Firewall can be used to diagnose such conditions by link and target address monitoring. Once the response of a remote target address to regular ICMP probing fails, the system can be configured to activate different routes and uplinks (for example, backup line, ISDN, xDSL). Through the use of this feature, traffic can still flow in unimpeded fashion across unaffected lines and crucial site-to-site and site-to-internet connectivity is still maintained.

ICMP Flooding, Type and Size Protection

To protect against ICMP-echo (ping) flooding, the Barracuda CloudGen Firewall allows you to configure a rate limit for ICMP echo packets. Packets arriving at a rate faster than allowed will simply be dropped. This also applies to the maximum allowed size of an ICMP echo packet (see: Forwarding Firewall Settings). ICMP echo packets, when they surpass the configured limit, are simply dropped by the firewall. You can also define on a per-firewall rule basis which other ICMP types will be propagated through the firewall.