Configuring Connection Limits on Cisco ASA Firewalls - Protect from DoS

The Cisco ASA firewall offers excellent protection for Denial of Service attacks, such as SYN floods, TCP excessive connection attacks etc. Using the new Policy Framework functionality, the ASA administrator can configure granular controls for TCP Connection limits and timeouts. For example, we can control and limit the maximum number of simultaneous TCP and UDP connections that are allowed towards a specific host (or subnet), the maximum number of simultaneous embryonic connections allowed (for SYN flood attacks), the per-client max number of connections allowed etc.

Configuration Example

STEP1: Identify the traffic to apply connection limits using a class mapASA(config)# access list CONNS-ACL extended permit ip any 10.1.1.1 255.255.255.255
ASA(config)# class-map CONNS-MAP
ASA(config-cmap)# match access-list CONNS-ACL

STEP2: Add a policy map to set the actions to take on the class map traffic

ASA(config)# policy-map CONNS-POLICY
ASA(config-pmap)# class CONNS-MAP
! The following sets connection number limits
ASA(config-pmap-c)# set connection {[conn-max n] [embryonic-conn-max n]
[per-client-embryonic-max n] [per-client-max n] [random-sequence-number {enable | disable}]}

where the **conn-max** n argument sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 65535.

The **embryonic-conn-max** n argument sets the maximum number of simultaneous embryonic connections allowed, between 0 and 65535.

The **per-client-embryonic-max** n argument sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 65535.

The **per-client-max** n argument sets the maximum number of simultaneous connections allowed per client, between 0 and 65535.

! The following sets connection timeouts
ASA(config-pmap-c)# set connection timeout {[embryonic hh:mm:ss] {tcp hh:mm:ss
[reset]] [half-closed hh:mm:ss] [dcd hh:mm:ss [max_retries]]}

STEP3: Apply the Policy on one or more interfaces or Globaly

ASA(config)# service-policy CONNS-POLICY {global | interface interface_name}

Source from: http://www.cisco-tips.com/configuring-connection-limits-on-cisco-asa-firewalls-protect-from-dos/