

Open Connection Attacks

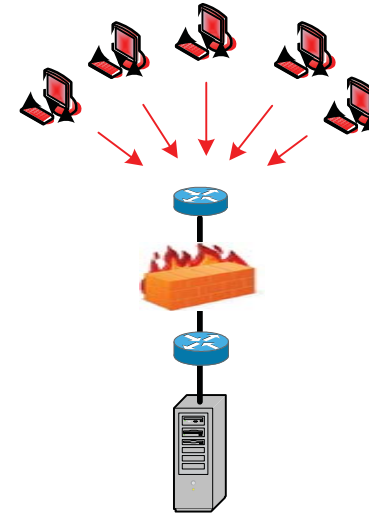
Protecting web servers from resource starvation

Open Connection attacks are a form of resource starvation attack in which bots are directed to establish and keep open TCP connections with a web server. This fills the web server software's connection table so that further requests cannot be served and legitimate clients are unable to connect. The attacks can take a few basic forms.

- *Attacks in which bots leave connections idle.* These can be mitigated with a firewall configured to enforce connection limits and aggressive idle time time-outs, which will close most of the bots' connections. In theory the web server software could close idle connections, however it is unclear whether any commonly used application implements this.
- *Attacks in which each of a relatively small number bots attempts to establish a large number of connections.* These can be mitigated with a firewall that limits the number of connections that each client can establish, which will block the majority of connection attempts.
- *Attacks in which each of a large number bots attempt to establish a large number of connections.* These cannot be mitigated by firewalls, since the firewall will allow more connections than the web server can handle. However, attempting to establish a large number of connections is blatant aberrant behavior that a few of the better dedicated anti-DDoS appliances on the market should be able to detect and deal with.
- *Attacks in which bots use the connections they've established, and do not each attempt to establish a large number of connections.* Traffic from these bots appears just like that from genuine clients: there are no idle connections to close, nor apparent misbehavior to detect. Under these circumstances even the best anti-DDoS appliances looking for misbehaving clients will have extreme difficulty distinguishing between bots' and legitimate clients' connections.

IntelliGuard's DPS series appliances have no such difficulty distinguishing between bots' and legitimate clients' connections. They employ a unique design that provides inherent strong protection against all types of connection attacks by way of independent monitoring of traffic to each server, configuration of limits, and automatic dropping of the least legitimate traffic when a server is at threat of being overwhelmed. In addition to this inherent protection, a number of specific server protection techniques are used, including limiting connection rates and number of simultaneous connections per server, authenticating the connections, and semi-automatic blacklisting of sources based on discovered commonalities between attack packets.

Few Bots, Many Connections

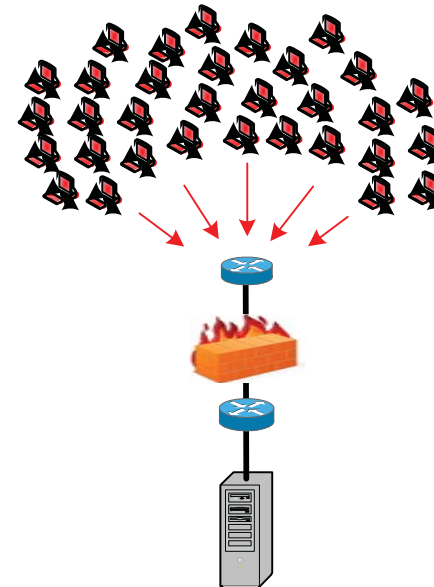


Few Bots
Attempt to establish many connections each

Firewall
Prevents Bots establishing more than a few connections each

Web Server
Handles all connections

Many Bots, Few Connections



Many Bots
Open few connections each

Firewall
Allows each bot to establish connections

Web Server
Overwhelmed with connections