DDoS Mitigation Service

Connectivity is everything for a web or application server—site or service users must be able to reach the server and get acceptably quick responses to their page or application requests. Most of the time, well-managed servers have plenty of bandwidth and service capacity, and increases in demand can be accommodated as needed. But connectivity bandwidth and server capacity can be exploited to effectively take the website or service offline, using a malicious method that is almost impossible to block at the server itself.

A **distributed denial-of-service** or **DDoS** attack occurs when multiple internet users flood the bandwidth or resources of a targeted web or application server. An attack from one source can be easily detected and blocked, but a distributed attack uses more than one unique IP address or source system, often from thousands of host computers infected with malware. Such malware can lie dormant for months or even years until triggered into action by a malicious entity. The sudden and persistent flood of service requests from such a "botnet" (robot network) can effectively block a site from normal access and cannot be easily thwarted by site filtering or user rejection. The targeted site will be effectively offline until the attack ends. A DDoS attack often fills the entire bandwidth of connectivity to a site or server and has been seen to reach multiple terabytes (1000 gigabytes) in scale against large server arrays.

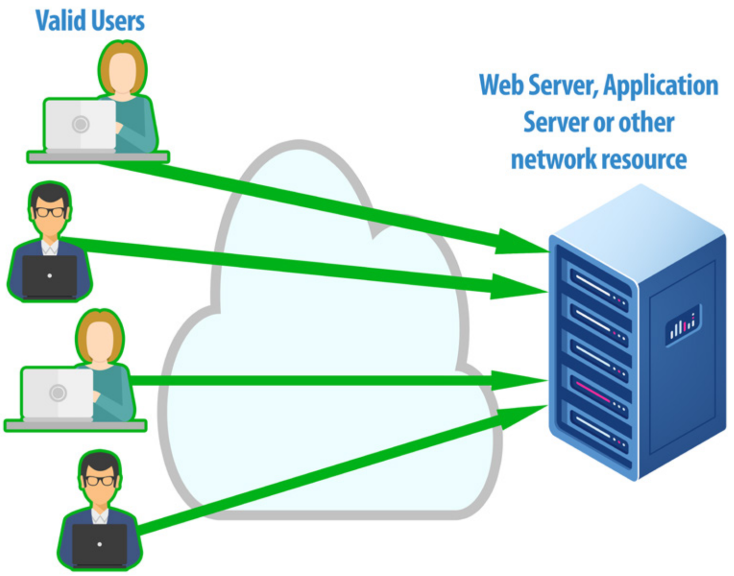
AireSpring DDoS Mitigation Service

AireSpring provides a FREE DDoS mitigation service for its Managed SD-WAN solution that utilizes either VMWare SD-WAN by VeloCloud™ or Fortinet SD-WAN for in-tunnel AireSpring IP addresses traversing the Airespring Gateway. AireSpring's DDoS Mitigation Service adds a layer of defense to your network that protects against the typical forms of a DDoS attack: HTTP floods, volumetric attacks, and bot-orchestrated flood attacks. It works by creating a separate tunnel in the public internet and re-routing all traffic to the targeted site, often using a far larger bandwidth than the site itself to contain and redirect the 'flood.' At the other end of the tunnel, "scrubbing" servers with massive capacity analyze the requests and reject those that match bot and attack profiles, but redirect valid requests to the original server. With such mitigation, most legitimate users will never know a DDoS attack is underway.

How It Works

When a customer notifies AireSpring of a possible DDoS attack, AireSpring's Network Operations Center (NOC) will investigate. If an actual DDoS attack is occurring, AireSpring will to the best of its ability reroute the customer's inbound traffic traversing their AireSpring SD-WAN to AireSpring's DDoS scrubbing centers, from which legitimate traffic will be forwarded on to the customer site.

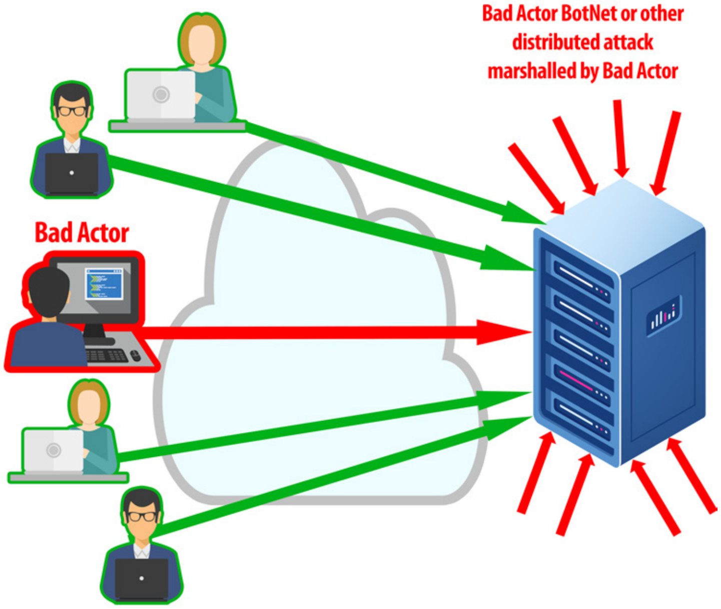
Normal access for up to hundreds of thousands of legitimate users.



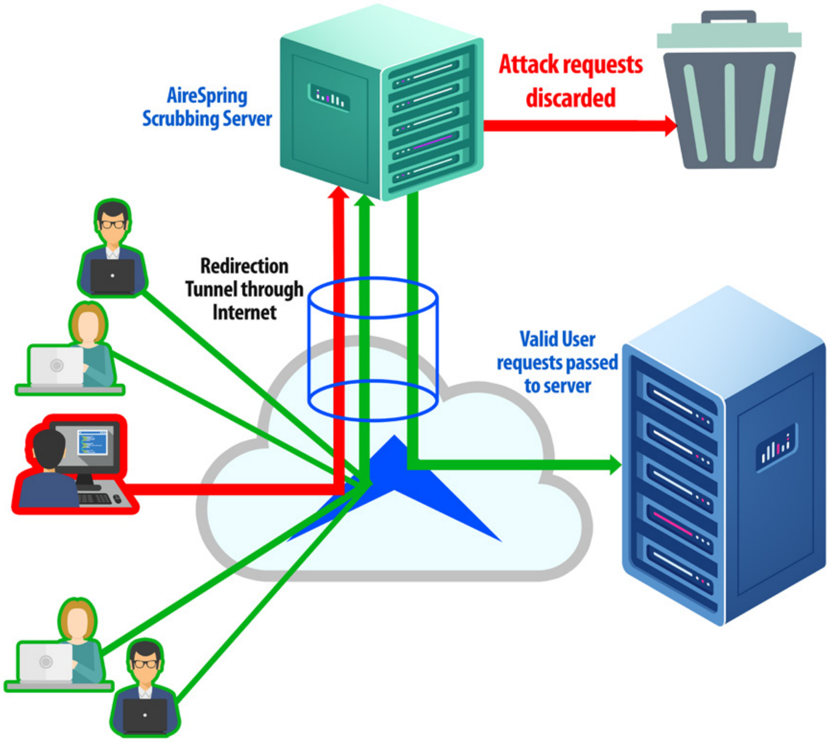
DDoS Mitigation Service

airespring®
Cloud, Fully Managed and Connected

Bad Actor triggers thousands of malware-infected systems to make repeated "empty" requests of server under attack. Legitimate user requests are lost or ignored in the flood, leaving the server essentially offline.


Bad Actor BotNet or other distributed attack marshalled by Bad Actor
Bad Actor

All traffic redirected to AireSpring scrubbing server through high-bandwidth tunnel. Legitimate user requests are identified and redirected to server while attack requests are discarded. Most users experience only slight delays in server response.


AireSpring Scrubbing Server
Attack requests discarded
Redirection Tunnel through Internet
Valid User requests passed to server

Ready to find out more? Contact us at 888-389-2899, email: sales@airespring.com, or visit our website at www.airespring.com

AT&T Partner Exchange
Solution Provider
PLATINUM ELITE