Secure DDoS Protection

Cisco Partner
https://cs.co/1page

Cisco **Secure DDoS Protection** solutions defend organizations against today's most sophisticated DDoS attacks using advanced behavioral-based and machine learning algorithms to rapidly detect and mitigate both network-layer (L3/4) and application-layer (L7) attacks.

Benefits:

Zero-Day DDoS protection: Patented adaptive, behavioral-based algorithms, continuously refined over the past decade, block sophisticated never-before-seen (zero-day) attacks with the lowest false positive rate in the industry.

Highest availability under attack: Accurately distinguishes legitimate from malicious traffic, enabling advanced SLA and maximizing service availability.

Increased data center efficiency: Comprehensive DDoS protection enables predictable engineering for network and application resources by eliminating anomalous flows that consume resources and impact application availability.

Deployment Options:

On-Premise DDoS Protection:
- Integrated with Cisco Secure Firewall 4100 & 9300 platforms.
- Virtual for private/public instances
- Dedicated on-premise appliances.
- Options include threat intelligence and SSL traffic inspection.

On-Demand Cloud DDoS Protection:
- Traffic diverted in case of large volume attack (Auto/Manual/API).
- Detection based on: NetFlow statistics, SNMP monitoring, *AWS* and *Azure* telemetry and third-party detection.

Always-on Cloud DDoS Protection:
- Traffic always routed through scrubbing centers.
- Real-time DDoS detection and mitigation by scrubbing centers.
- Available for all Networks.

Hybrid DDoS Protection:
- On-premises mitigation appliances with on-demand cloud protection.
- Real-time detection and mitigation done locally.
- Mitigation diverted to cloud before pipe saturation.

Features:

A few of the protections now available to Cisco customers:

- Anti-Scanning Protection
- Burst-Attack Protection
- Carpet-Bombing Protection
- Connection PPS Protection
- HTTPS Flood Protection
- Subscription services:
  - Geolocation Protection
  - ERT Active Attackers
  - Security Update Service (SUS)
- Traffic Filters

[1] Cisco partners with Radware. DefensePro is a registered trademark of Radware.

FAQs:

Why would someone carry out a DDoS attack?
There are many motives from disruption of services to espionage and cyber warfare:
- Make a political statement (hacktivism)
- Disrupt communications and essential services
- Gain a competitive advantage
- Achieve financial gain through extortion, theft, etc.
- Inflict brand/reputational damage
- Steal or destroy confidential information or intellectual property
- Launch a ransomware attack
- Wage cyber warfare

Which industries are being targeted by DDoS and why?
While DDoS attacks are a threat to all businesses, DDoS attacks most often target the:
- **Online gaming and gambling:** To win a competitive advantage or financial gain.
- **Service providers:** To commit data theft, eavesdrop, disrupt essential services, or inflict reputational damage.
- **Cloud services** (AWS, Azure, etc.): To commit data theft, eavesdrop, disrupt essential services, or inflict reputational damage.
- **Governments/SLED:** To steal intellectual property, disrupt operations, eavesdrop, commit espionage, or gain a competitive advantage.
- **Financial services:** To achieve financial gain, inflict reputational damage, access confidential data, or cause disruption.
- **Online retailers:** To disrupt operations, gain a competitive advantage, inflict reputational damage, or steal intellectual property.
- **Healthcare:** To disrupt services, inflict reputational damage and extort for ransom.

How long does a DDoS attack last?
DDoS attacks can vary. Attacks like the *Ping of Death* can be short. The *Slowloris* attack takes longer to develop. According to a Radware report, 33 percent of DDoS attacks last an hour; 60 percent last less than a full day; and 15 percent last as long as a month.

Resources:

SalesConnect
NetSec Ordering Guide
Cloud DDoS Order Guide
At-a-Glance
DefensePro® Data Sheet
4100 Series Firewalls
9300 Series Firewalls
Cisco Secure ACD
Advanced WAF & Bot Protection
What is a DDoS Attack?
5 Steps for protection
Public page

Example SKU: ***DDOS-SEC-SUB***