Cloud DDoS Protection

Protect your organization from DDoS attacks.

DDoS attacks result in loss of revenue, loss of customers, disruption of service availability, damage to brand, theft of vital data, and more. With internet access now a critical component of any business, it is disastrous for enterprises to shut down services and wait for any attack to subside. Prevent all DDoS attacks by deploying MetTel's Cloud DDoS Protection service.

Key Benefits

WIDE RANGE OF ATTACK PROTECTION

MetTel's Cloud DDoS Protection provides a wide range of mitigation policies and algorithms capable of defeating L3/L4 and L7 DDoS attacks, regardless of their size, frequency duration, and complexity.

DELIVERING CLEAN TRAFFIC

Our solution provides flexible "clean traffic re-injection" options when connecting to the cloud. Due to traditional GRE approaches being less reliable, MetTel provides direct access within a common data center or reliable access to over 150 data centers globally.

FUTURE READY (IPV6 CAPABLE)

Our DDoS system is ready to support and provide protection for your critical infrastructure, before, during and after your migration to IPv6.

Features

COMPLETE PROTECTION

Our cloud DDoS solution lets you regain control and confidence with our layered protections from sophisticated attacks today.

ON-DEMAND & AUTOMATED

We have developed a large-scale DDoS cloud infrastructure that leverages purpose-built, carrier-grade DDoS protection appliances with the industry's lowest false positives.

LOCAL TRAFFIC WITH REMOTE SCRUBBING

We offer remote DDoS scrubbing capability that absorbs attack traffic at the source while ensuring local traffic is unaffected and is not re-routed, which would incur additional latency.

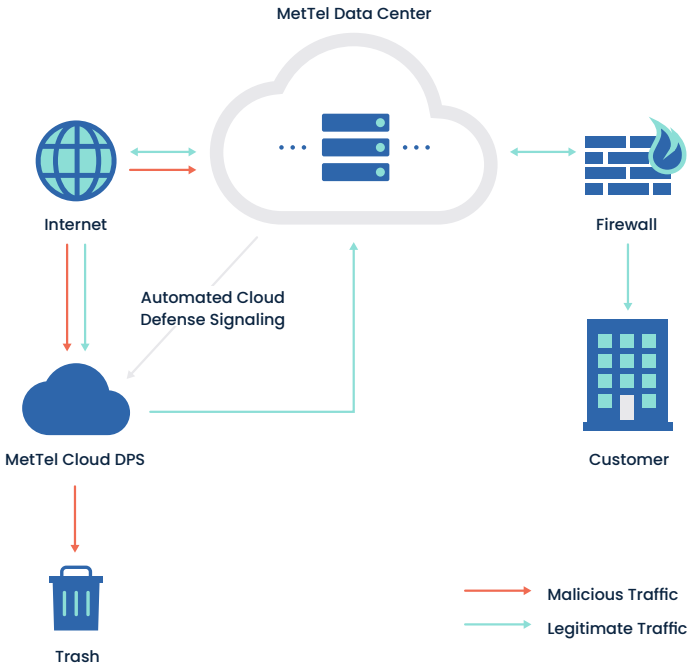
TRANSPARENT DDOS SCRUBBING

We designed our solution to flex with the attack volume and duration and can absorb attacks that exceed multiple terabytes.

For more info, contact your MetTel agent or visit mettel.net.

Cloud DDoS Protection Solution

MetTel utilizes a unique hybrid approach to defeat the damaging effects of DDoS attacks. The approach combines MetTel on-premises defenses with the on-demand MetTel Cloud DDoS Protection service. Working in unison, the solution eliminates smaller/shorter attacks on-premises, while defending infrastructures against bandwidth saturating DDoS attacks using the MetTel cloud. Both defenses are fully integrated resulting in increased bandwidth visibility, reduced cloud redirect times for mitigation, and coverage for all L3-L7 DDoS attack vectors.



In the above scenario, the defenses are designed to defeat all DDoS attacks that are under the available internet bandwidth. The defenses also monitor a host of attributes and can easily detect conditions that indicate an impending bandwidth saturation attack. In this instance, the data center DDoS defenses signal the MetTel Cloud DDoS Protection via an always-on BGP session with the cloud. This signal effectively instructs the MetTel Cloud to reroute all incoming traffic through the cloud centers for the IP address under attack.

Three Stage Approach

We focus on a three-stage approach that monitors, detects, and mitigates the most complex DDoS attacks, ensuring only legitimate traffic reaches important network and application.

1. MONITORING

The Cloud DDoS Protection is easily deployed in any network and can scale to support hundreds of Gbps of inspected traffic. It monitors in real-time and supports the full suite of IP protocols necessary to ensure complete network visibility.

2. DETECTION

At the heart of the Cloud DDoS Protection is an innovative, multi-stage detection engine. All packets are subjected to a series of algorithms and other defense mechanisms to accurately identify malicious traffic. These include RFC checks, protocol analysis, access control lists, IP reputation, anti-spoofing, L4-L7 algorithmic analysis, user behavior analysis, regular expressions, and connection/rate limiting. Together they provide industry-leading accuracy that protects against both known and zero-day threats. The detection engine is optimized frequently, so you always have the most accurate protection available.

3. MITIGATION

Once malicious traffic has been identified by the Cloud DDoS Protection, it is removed, and the system forwards only legitimate traffic to its intended destination. Extensive reporting of DDoS attacks in real-time provides valuable information such as attack types, source/destination IPs, protocols, and more.

For more info, contact your MetTel agent or visit mettel.net.