iTel NETWORKS

DDoS Protection

DDoS Protection

Safeguarding Your Network, Resources, and Reputation

A DDoS attack floods your network or website with bot traffic, consuming available bandwidth and blocking your customers before crashing your network or site. As an iTel customer, DDoS Protection is seamlessly integrated into your internet service. iTel deploys, monitors and maintains the service on behalf of the customer to free up your resources for other tasks such as monitoring for breach and protecting against data theft. Preventing DDoS attack protects you from unwanted financial burdens as well as protecting your company's reputation

iTel managed templates for traffic alerting and mitigation

Automated attack response

24x7x365 iTel monitored alert and attack handling

iTel NETWORKS

What Is DDoS

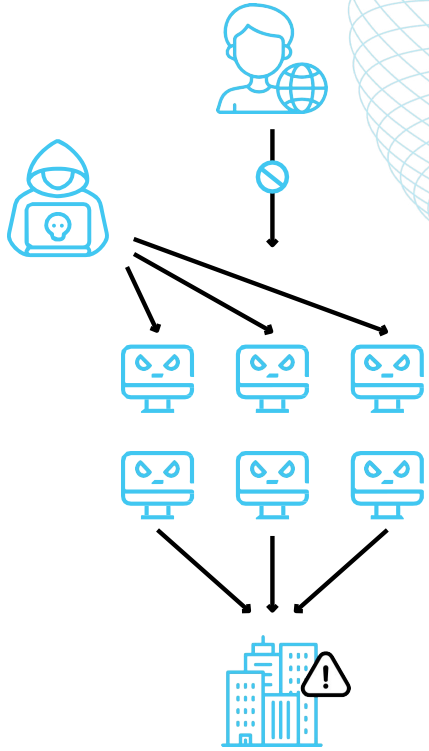
Protect Yourself And Your Clients

Have you heard of DDoS attacks? These are serious attempts to render a computer or network inaccessible to legitimate users. In Distributed Denial of Service (DDoS) attacks, multiple sources, often compromised devices, join forces to overwhelm the target. Picture this: during a volumetric DDoS attack, a target's internet pipe gets bombarded with an overwhelming flood of requests from Botnets. These requests saturate the network, causing it to stop responding and blocking genuine traffic.

Botnets are networks of thousands of compromised devices, including computers, servers, and IoT devices. They simultaneously bombard the target with multiple requests, amplifying the traffic across the internet. Within seconds, the target's internet connection and devices become useless, rendering them powerless. DDoS attacks can be purchased for as little as $5 USD per hour on the dark web.

The consequences of DDoS attacks are severe. On average, SMBs face a $123,000 impact, while enterprises endure over $2,000,000 in losses. Attacks not only harm finances but also damage brands, erode customer trust, and risk data theft.

Don't let your business fall victim to these malicious attacks. With our comprehensive DDoS protection services, you can safeguard your network, reputation, and valuable assets. Stay one step ahead of attackers and ensure uninterrupted service for your customers.



iTel NETWORKS

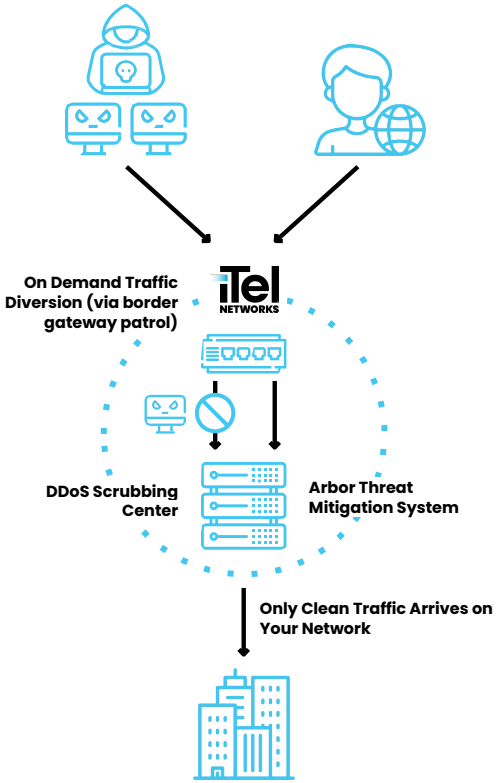
How Does DDoS Protection Help?

Defending Against DDoS Attacks: Protect Your Network

DDoS attacks pose unique challenges, as they originate from global botnets with compromised connections that may appear legitimate. Firewalls alone cannot effectively block these attacks, as the overwhelming traffic quickly fills the access pipe, causing connection drops and delays. The cycle of overwhelming and resetting continues, creating a recurring DDoS attack scenario.

Our Volumetric DDoS protection tackles this issue head-on by specifically targeting and removing malicious traffic before it floods your network devices and servers. With our proactive monitoring and support solution, we mitigate DDoS volumetric attacks within our network, ensuring they never reach your infrastructure. This prevents your access pipe from overflowing and keeps your operations running smoothly.

As a managed service, we tailor the protection to your network's normal traffic patterns. Any deviations trigger immediate alerts, and we initiate automatic mitigation within 300 seconds. Our team keeps you informed throughout the attack, monitoring for any changes in attack vectors. This frees up your security team to focus on detecting other potential issues, such as attempted data breaches.



iTel NETWORKS

Volumetric Attack Handling

Advanced Volumetric Attack Handling: Robust Protection for Your Network

iTel's DDoS Protection provides robust volumetric defense, automatically redirecting and mitigating traffic when it surpasses a certain threshold. Our advanced system detects and mitigates attacks, ensuring that only clean traffic reaches your network. With iTel managing traffic templates and monitoring for attacks, your resources can focus on crucial tasks.

When an attack occurs, our dedicated team receives instant alerts. If the attack exceeds a specific threshold, auto-mitigation kicks in within 300 seconds. Our assurance team, available 24/7/365, diligently monitors the ticket queue. Upon receiving a ticket, they promptly investigate the situation and notify authorized contacts if needed. Throughout the attack, the assurance team continually monitors and manually intervenes if necessary.

Say goodbye to disruptive volumetric attacks. Trust iTel's advanced protection to safeguard your network, while our expert team handles the complexities. Focus on what matters most, as we keep your operations secure and running smoothly.

Attack Type	Detect	Mitigation
Below 49 GBPS Attack	Y	Y
Above 49 GBPS Attack	Y	Y
Low And Slow Attacks	N	Some*
Layer 7	N	Some*
UPD Flood	Y	Y
ICMP Flood	Y	Y
SYN Flood	Y	Y
NTP Amplification	Y	Y
HTTP Flood	N	Some*

*The iTel scrubbing centre has some mitigation techniques against HTTP Floods, so depending on the attack it may be able to resolve some Low and Slow and Layer 7 attacks. However, to mitigate these types of attacks, a mitigation must have been started prior to the event (due to a pre-existing volumetric attack, or manual intervention). There is no detection for application-layer attacks to automatically mitigate these attacks.

iTel NETWORKS

Service Level Objectives

Measure	Indicator	Service Level Objective
Time to Commence Automitigation	Attack must meet volumetric parameters. Clock starts from when threshold alert is triggered and runs until customer bound traffic is directed into the scrubbing centre.	300 Seconds 24/7 Support
Helpdesk Attach Alert	Elapsed time from start of attack to time when ticket is picked up in the queue by iTel support staff	15 min 24/7 Support
Helpdesk Notification of Attack Completion	Elapsed time from the completion of the attack to when customer receives the first alert call	60 mins after completion of the attack* 24/7 support
Helpdesk Support for Emergency	Elapsed time from reception of the Customer's call as a trouble ticket for DDoS attack causing network failure	30 mins** 24/7 support
	Elapsed time from notification back by iTel to completion	60 mins after completion of the attack* 24/7 support

DDoS Protection Service Clock Stop Conditions

Issue	Specific Condition
Time to Commence Automitigation	Periods scheduled by iTel for maintenance or upgrades which cause downtime or lower capacity. Any such Clock Stop Condition shall not extend beyond the scheduled period of the maintenance or upgrade. Service Level Metrics apply for any outage beyond the scheduled maintenance or upgrade period.
Even Of Force Majeure	Periods during natural catastrophes that interrupt services delivery.

iTel NETWORKS

Notes:
*As the length of a DDoS attack is unpredictable, iTel commits to monitoring the attack and will inform the customer within a certain period of time once the attack completes
**Issue must have been verified to be due to a DDoS attack and not caused by other outages

iTel Authorization Contact List

In order for iTel to best serve you, it is absolutely critical that you keep your contact information up-to-date. Current Authorized Contacts are the only people who can modify your customer contact information. Over time, people move and postal addresses, email addresses, pager numbers, or phone numbers change.

It is extremely beneficial for you to inform us of these changes, so we know whom to contact at your company about urgent issues or if a non-authorized person requests service. Please contact your Account Executive or email cs@itel.com for any contact changes.

iTel Responsibilities

- Administration of scrubbing centre
- Monitoring (UP/DOWN) with incident created
- Troubleshooting incidents
- Software Release / Patch Management
- Hardware upgrades
- Threshold policies

Client Responsibilities

- Customer information kept current

iTel NETWORKS

Connecting
Everything