iTel networks inc

DDOS PROTECTION

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

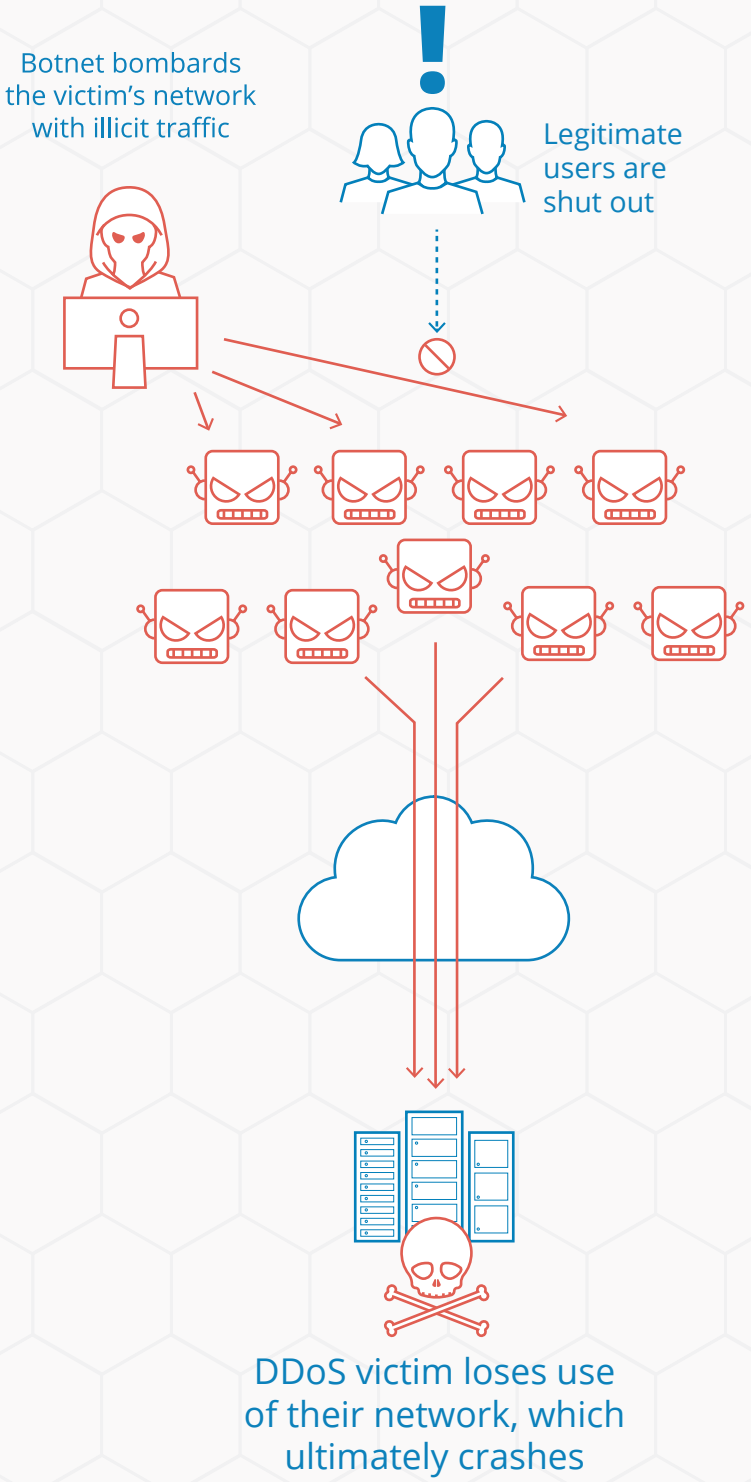
Automated attack response

24x7x365 iTel monitored alerts and attack handling

WHAT IS DDOS?

Denial of Service attacks are attempts to flood the target's network to make a computer or network unavailable to legitimate users. In Distributed Denial of Service (DDoS) the attacks are coming from multiple sources, mostly comprised of compromised devices. For example: during a volumetric DDoS attack a target's internet pipe is bombarded with a massive volume of requests from Botnets that saturate their network which results in the network no longer responding and blocking legitimate traffic. Botnets are made up of thousands of compromised internet connected computers, servers or IOT devices, which simultaneously sends multiple requests to a target, further aggregating the traffic over the internet, swamping the target's internet connection and devices, rendering them useless within seconds.

The sponsor or initiator of the attack is rarely the same person that conducts it. Typically they pay an unrelated attacker to initiate and control the attack. It's possible to buy a DDoS attack on the dark web for as little as $5USD an hour. The average financial impact of a single attack for a SMB is $123,000 and over $2,000,000 for an enterprise. In additional to financial burdens, the company may suffer from brand damage, loss of customer trust, loss of data and intellectual property. Not all DDoS attacks are meant to disrupt the service. Some attacks are used as a smoke screen to occupy the target's security team while the attacker steals data or perform other criminal activities.



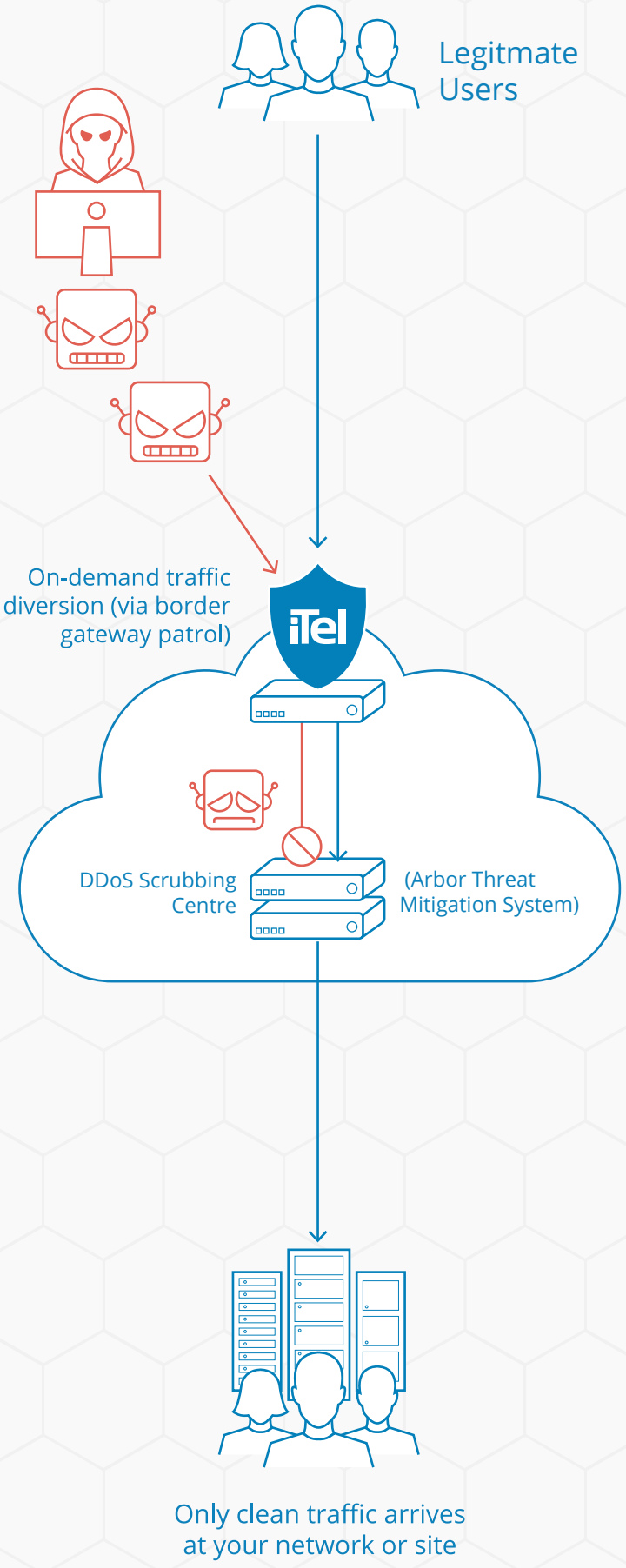
HOW DOES DDOS PROTECTION HELP?

Due to the nature of DDoS, it's not possible to use a firewall to block the attack because it's coming from botnets all over the world and each compromised connection may be a legitimate user when it's not being used as an attack tool.

Even if the firewall can perform some blocking features, once the access pipe in front of the firewall is filled, additional traffic will be dropped. When the firewall is overwhelmed, it usually stalls or resets which drops the entire connection. A firewall reset may take up to several minutes before it can start re-receiving connections, only to be overwhelmed again. This is a common occurrence for a DDoS attack.

Volumetric DDoS protection specifically targets the attack and removes unwanted traffic to prevent the access pipe from overflowing and overwhelming network devices and servers. The attack traffic is redirected in the provider network before it can reach the target's network. Traffic is then scrubbed and only clean traffic is forwarded to the client.

iTel DDoS Protection is a proactive monitoring and support solution which provides mitigation against DDoS volumetric attacks. This protection happens in the iTel network so the attack will not reach the client network. This will prevent the client's access pipe from overflowing. As a managed service, iTel will determine parameters for your normal network traffic profile. If traffic ever deviates from these patterns, iTel will receive alerts and provide auto-mitigation within 300 seconds. iTel will inform the customer when an attack happens and continue to monitor the attack in case the vector changes. This alleviates the client's security team from monitoring the DDoS attack and instead they can focus on detecting other potential issues like an attempted data breach.



VOLUMETRIC ATTACK HANDLING

iTel's DDoS Protection offers volumetric protection – once traffic reaches a certain level, it will be redirected to the scrubbing centre to mitigate. This action involves the ability to detect the attack and the ability to mitigate the attack. Once the traffic is scrubbed, the clean traffic will be forwarded to your network. iTel will maintain the traffic templates and monitor for attacks on your behalf, freeing up your resources for other important tasks.

When a customer is under attack, the iTel team will receive an Alert. If the attack passes a certain threshold, auto-mitigation starts within 300 seconds. The ticket queue is monitored by the assurance team 24x7x365. Once the ticket is received, they will investigate the situation and, if necessary, will inform the authorized contact about the attack. The assurance team will monitor the attack and manually intervene if necessary.

	DETECT	MITIGATE
BELOW 40GBPS ATTACK	Y	Y
ABOVE 40GBPS ATTACK	Y	Y
LOW AND SLOW ATTACKS	N	Some*
LAYER 7	N	Some*
UDP FLOOD	Y	Y
ICMP FLOOD	Y	Y
SYN FLOOD	Y	Y
NTP AMPLIFICATION	Y	Y
HTTP FLOOD	N	Some*

*The iTel scrubbing centre can 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.

SERVICE LEVEL OBJECTIVES

The Service Level Metrics for the iTel DDoS Protection Services ("iTel DDoS Protection Service Level Metrics") including measurement methodologies are detailed below.

MEASURE	INDICATOR	SERVICE LEVEL OBJECTIVE:
TIME TO COMMENCE AUTO-MITIGATION	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 ATTACK ALERT	Elapsed time from start of attack to time when ticket is picked up in the queue by iTel support staff	15 mins 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
SCHEDULED MAINTENANCE	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 shall apply for any outage beyond the scheduled maintenance or upgrade period.
EVENT OF FORCE MAJEURE	Periods during natural catastrophes that interrupt services delivery.

iTel reserves the right to execute emergency changes to ensure Service Availability without prior customer approval.

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

ROLES AND RESPONSIBILITIES

iTel Responsibilities	Client Responsibilities
• Administration of scrubbing centre • Monitoring (UP/DOWN) with incident created • Troubleshooting incidents • Software Release / Patch Management • Hardware upgrades • Threshold policies	• Customer information kept current

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.