IMPLETEC

Ubiquitous
Reliable
Uninterrupted
Delivery

iCore
DDoS Mitigation Stack

There are times, when an online business' operation can grind to a halt because of DDoS attacks. There are also times, when the protection services of proxy-shield DDoS Mitigation vendors are inapplicable. Be it because of lag and latency issues associated with such services, or simply because of internal strategic requirements of your establishment.

These are the times, when you need an in-house solution that is stationed in your own DC and you are in charge of its operation. With linear scalability and comprehensive configuration and customization flexibility, the iCore Mitigation Stack is here to give you the fulll-bodied, industry-leading Layer 3 to 7 protection you need.

WHY ON-PREMISE MITIGATION?

Although perimeter security configurations, such as intrusion prevention systems (IPS) and firewalls are critical components of traditional layered-defense approaches, they are not intended to cope with DDoS attacks. Firewalls are widely used to execute access-governing policies to on-site resources, while IPS's deal with all kinds of malware, blocking it from infecting end-systems or exploiting certain vulnerabilities. The DDoS threat is a whole new ballgame.

DDoS attacks are launched from multiple sources sending legitimate traffic, aiming to deplete availability-critical resources, such as bandwidth allocations, session and application service capacity (e.g., HTTP/HTTPS, DNS) or causing back-end database overload. Stateful in-line devices, such as Firewalls and IPS's are not designed to block or even withstand DDoS traffic. Such traffic simply floods these devices. It is a well known fact that DDoS attacks are frequently orchestrated to target precisely these devices in an attempt to pave the way for additional hacking attempts aimed at stealing or destroying data from deeper in the protected resource.

What needs to come into play to meaningfully tackle the DDoS problem is a different breed of security solution, and that is the iCore DDoS Mitigation Stack.

The business case for on-premise DDoS Mitigation implementation is simple indeed. Although this approach involves investment that is considerably higher than using outsourced proxy-shield services, it comes with a whole set of advantages that make up for the difference in price:

- your traffic does not go through scrubbing centers for filtering, but comes directly into your own Data Center, eliminating any latency/lag issues associated with proxy mitigation and the additional rerouting involved
- you gain full control over the mitigation process, including traffic usage data collection, raw attack statistic derivation and lists of blocked IP's (where applicable) for forensic analysis
- the stack is used only by you (with proxy services you're often on a shared structure), thus you have a truly bespoke solution to adhere to internal traffic policies
- the iCore provides linearly scalable mitigation, allowing incremental protection power increase when you need it
- if you are running a hosting business - the stack enables you to sell DDoS Protection to customers, under your own business model
- total security and manageability with your own trusted staff trained by us, or with our vetted 24/7 fully-qualified support team

GET IN TOUCH WITH US

Impletec Technologies Ltd
4 Lale Street, Lozenetz Dist., 1421 Sofia, Bulgaria
ph. 359 2 442 0451, fax 359 2 866 1812

www.impletec.com

TYPICAL CLIENTS of iCORE

In our experience dealing with the DDoS plague, we have identified three major client groups that could benefit most from our iCore DDoS Mitigation Stack. Based on specific requirements and needs in DDoS protection, they are:

GOVERNMENT

- Ensure overall network availability and security by proactively detecting and mitigating DDoS attacks, identifying and blocking botnets where applicable and gathering forensic evidence in the fight against attackers
- Become knowledgeable and gain real-time visibility into current and evolving internet-borne network threats
- Obtain the intelligence necessary to take measures to reduce organizational risk and defend from malicious traffic attacks
- Adequately address regulation issues and comply with various compliance requirements and guidelines of regulatory bodies and policies on information security and resource protection

ENTERPRISES

- Ensure critical service availability and uninterrupted operation for internet-intensive business applications: Web, e-commerce, email and others
- Access and compile your own data on emerging global and industry-specific Internet threats
- Gather actionable intelligence to assemble and deploy the optimal defenses to ensure the enterprise's network front-line security
- Detect and mitigate the DDoS threat to secure protection of your company's intellectual property and trade secrets from further hacks aimed at theft or damage inflicted by advanced network threats or internal network deliberate or inadvertent misuse

SERVICE PROVIDERS

- Ensure proper detection and mitigation from DDoS attacks so service availability is secured as well as critical network operations and infrastructure
- Increase operational efficiency and achieve cost-reduction through far-reaching insight into critical network-based operations and components such as routers, IP flow and Application-Layer data
- Deploy your own business model to effectively capture market demand trends for ultimate flexibility and self-sufficiency in service provision to clients.
- Be able to offer DDoS-free managed services and ultimately achieve improved customer satisfaction and increase in revenue streams

HOW DOES iCore WORK?

The iCore DDoS Mitigation Stack is a first-line-of-defense security solution for your entire Data Center or protected resource of choice.

Designed to withstand and mitigate all known and evolving types of DDoS attacks, the iCore filters all ingress traffic silently and swiftly to ensure critical application and resource availability and uninterrupted online operation.

The Stack is composed of several hardware devices running proprietary purpose-built Impletec software applications.

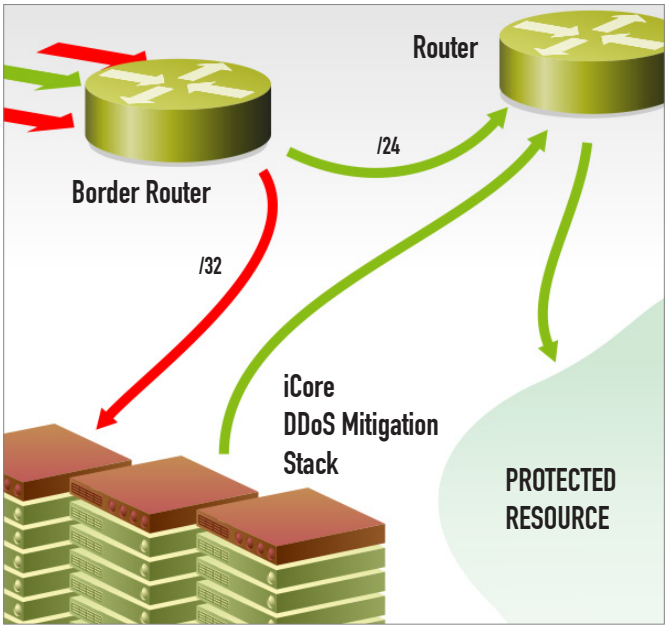
The underlying philosophy behind our solution is to effectively protect you from DDoS at the maximum possible speed, with minimal fail-positives.

The Stack runs on either of two operation modes:

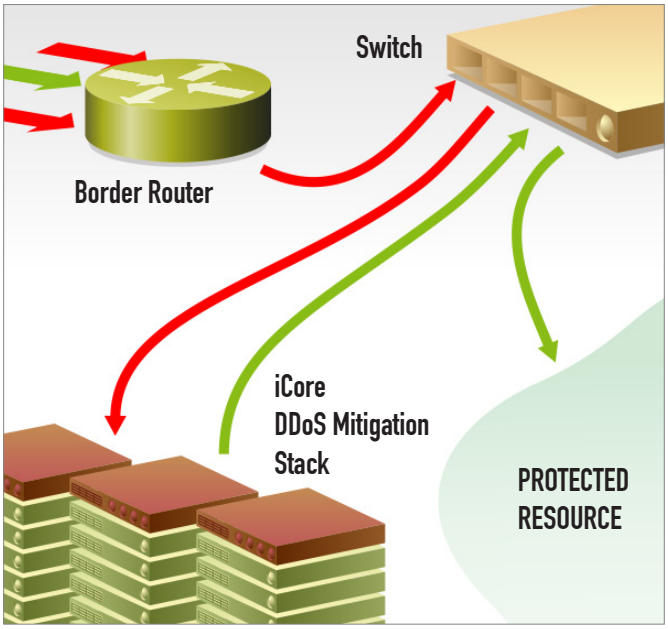
(i) "attack-free" mode – all traffic is routed directly to the receiving resource without mitigation applied; only round-the-clock monitoring and detection applications running to ensure actionable system response if/when it comes under a DDoS attack, and

(ii) "under-attack" mode – traffic to the protected resource is routed through the mitigation components of the Stack, where it is cleaned, filtered (in several stages and with several filter levels corresponding to attack type and severity), analyzed and intrusion statistics recorded. Cleansed traffic is then proxied to the receiving protected resource.

There are two basic "styles" of making the iCore part of your network. One involves a network router device and the other, a switch. The decision on which to implement depends entirely on customer's existing infrastructure or is simply a matter of choice.



"Attack-free" mode: traffic passes through the routers directly. "Under-attack" mode: traffic to attack destination is routed for cleaning to iCore by sending /32 BGP-Announcement (preferred route) to Border Router. As the attack ceases, the /32 BGP-Announcement is removed.



"Attack-free" mode: traffic is routed through the switch directly to protected resource. "Under-attack" mode: route is modified by the iCore's detector (ARP-flow) to the switch. Thus, DDoS traffic enters the iCore for cleaning. Once the attack stops, routing is switched back to direct mode.

GET IN TOUCH WITH US

Impletec Technologies Ltd
4 Lale Street, Lozenetz Dist., 1421 Sofia, Bulgaria
ph. 359 2 442 0451, fax 359 2 866 1812

www.impletec.com

MORE ON THE iCore

The iCore is designed and built to provide an extensive range of customizable options, so customers can tune the mitigation process and capacities to fit their specific needs.

FEATURES & CUSTOMIZATION

The stack is managed through an individually brandable Control Panel (CP) with an all-browser web-based interface. With comprehensive access-level management, the Panel is suitable for administrators and end users alike. The CP provides setup/modification access as well as filter and mode management.

Applying special rules, providing additional ports for proxying of clean traffic, permanent whitelist management (important for CMS and Search Engine bots unhindered operation, for example) are just some of the capabilities one has access to when managing the iCore through the Panel.

SEARCH ENGINES & iCore

Search Engines (SE's) and their bots' unobstructed access to a website is important and we fully understand that. SE rankings are targeted through marketing strategies and are a symbol of status and high customer demand for a company's offerings.

What is it the iCore does so SE's don't get blocked? First of all, in contrast to the majority of other DDoS Mitigation solutions, the iCore does not filter traffic by default when there's no DDoS attack present. All traffic passes directly to the protected resource.

The Stack is designed to intelligently monitor traffic, especially on Application Layer, with filters OFF if there is no attack, and when "under attack" the filters are continually being adjusted in accordance with attack severity and size, either automatically or manually.

Second, for those times when your site comes under attack on Application Layer and the filters are ON, the iCore keeps permanent whitelists for all major search engines. As new SE crawler networks appear, the iCore is updated with that information remotely by Impletec or by your staff through the CP's permanent whitelist feature.

EMERGENCY ACCESS & UPDATES

DDoS attacks evolve constantly. So does the iCore. We keep it updated for you through remote access. Simple as that.

98% of today's DDoS attacks are automatically mitigated by the iCore Stack. The remaining 2% require qualified human intervention, which can be effected either remotely by us or by your own trained and qualified by Impletec staff.

HARDWARE

Impletec is prepared to supply the hardware for the implementation of the Stack, preconfigured with our industry-leading mitigation software solution. Alternatively, the customer may choose to deploy it on their own, existing hardware. In these cases, Impletec issues the customer with recommended configurations and hardware specifications to ensure desired solution operation.

SCALABILITY

The iCore is linearly scalable, providing customers with the option for incremental increase of mitigation capacities up to a certain bandwidth allocation, for example.

INTERESTED?

For further consultation, assessments and quotations as well as to receive a standard configuration Data Sheet of hardware supplied or recommended by Impletec, please contact us with your current network setup and specific requirements in terms of desired attack mitigation size and or existing bandwidth to be protected.