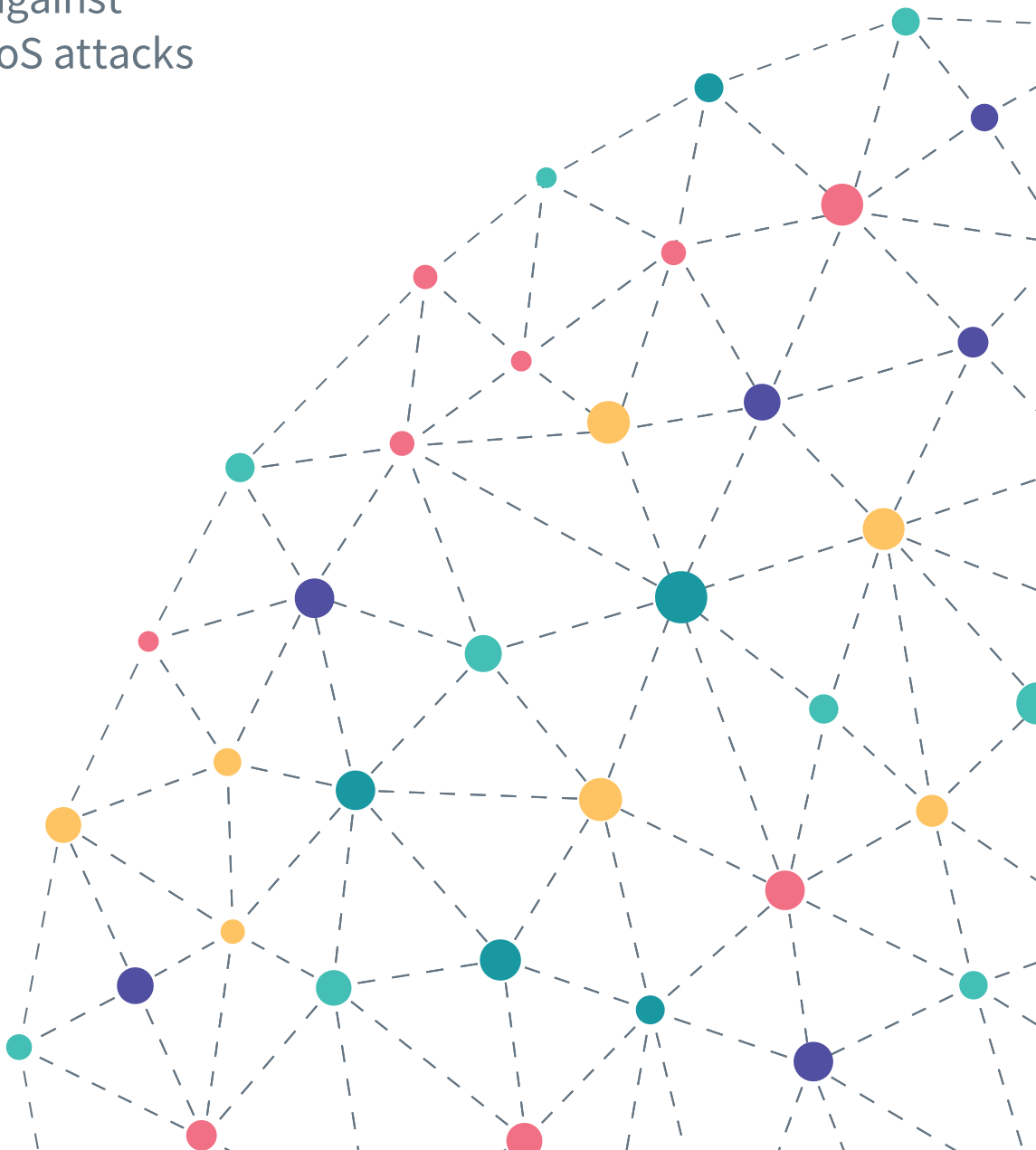
TELXIUS

Enabling Communication

A Telxius White Paper

Understand & protect

How to defend against the threat of DDoS attacks



01. Executive Summary

Denial of service attacks have become one of the primary cybersecurity threats facing enterprises, making DDoS protection an essential part of a cybersecurity strategy [1]

In the last decade, Distributed Denial of Service (DDoS) attacks have become an increasingly sophisticated and dangerous threat on the Internet that most companies face on a daily basis. According to research by Ponemon Institute, on average DDoS attacks cost companies $1.5 million annually.[2]

According to the Davos World Economic Forum, all organizations should assume they have been hacked, or at least agree that it is not a question of 'if' they will be targeted for an attack, but 'when'.

Given the rapid and extraordinary changes that have taken place in the DDoS landscape, companies now need to implement security measures that not only protect their clients' infrastructure but also their own network.

According to the Arbor Infrastructure Security Report 2014, the DDoS landscape has evolved as a result of a combination of factors:

- An increase in the number of attacks and wider use of 'quick hit' techniques which involve short, high-intensity attacks.
- Greater use of hosting and cloud facilities as launch points for DDoS attacks in order to circumvent detection and increase attack capacity.
- Higher frequency of application layer DDoS attacks both as a stand-alone technique and combined with volumetric attack methods.

This white paper will outline the consequences for your business of not preventing DDoS attacks. Grave consequences such as declines in productivity, damage to brand and reputation, and lost revenue.

In addition, it aims to provide in-depth insights into the way in which DDoS attacks are being carried out and how to protect your organisation – and your customers – against them. Crucially, it will help assess what an effective DDoS solution could mean for your business.

1 Source: http://www.stateoftheinternet.com/security-cybersecurity-ddos-protection-ddos-mitigation.html
2 Source: The Cost of Denial of Service Attacks, Ponemon Institute, March 2015.

02.
DDoS attacks – what are they?

"The increasingly complex nature of DDoS attacks is making effective detection and mitigation involve more than just deploying an appliance or service. Many organizations that do not have the ability to dedicate resources and skills to monitor and manage their DDoS risk exposure on a daily basis and are seeking increased context and value-added services from their providers for DDoS mitigation."

Source: Gartner Competitive Landscape: DDoS Mitigation Solutions 28 October 2014 G00261259 Gartner Analyst(s): Sid Deshpande, Principal Research Analyst | Eric Ahlm, Research Director

Distributed Denial of Service (DDoS) attacks are among the most common threats on the Internet. These attacks are generated internationally and their main task is to saturate network bandwidth to make the network unavailable to its intended users and prevent a service being provided.

Whereas in the past most attacks were random, today's are more systematic and often focus on a single organisation. An attacker's motivation can range from 'hacktivisim' and extortion, to competitive sabotage or even simple vandalism. Whatever the reason behind them, DDoS attacks are a global issue and no organisation can afford to ignore them.

2.1 Understanding attacks

DDoS attacks attempt to saturate your Internet links to make your service unavailable. By overwhelming the network with a high volume of traffic or opening a huge number of sessions that the network's resources are unable to bear, performance is reduced to an unusable level.

Fundamentally, there are two types of attacks. The first takes place at the application layer (Layer 7) and the second at the network layer (Layer 3):

- **Application layer:** attacks are especially worrisome for SaaS application providers. These attacks mimic legitimate user traffic to bypass barebone anti-DDoS solutions and crash the web server.

- **Network layer:** attacks bring down a website or SaaS application by overwhelming network and server resources, causing downtime and blocking responses to legitimate traffic.

DDoS attacks are often launched against victims by using a network of zombie machines or botnet.

It is important to understand that for attacks intended to consume available bandwidth, the only effective strategy is to mitigate the attack as close as possible to the source in order to prevent your Internet links becoming saturated.

Furthermore, if an attack successfully consumes a huge bandwidth and then saturates the network's international trunk links, all your customers could be harmed too. Consequently, the impact can go well beyond negative economic impact, leading to customer dissatisfaction and damaged brand reputation.

2.2 DDoS attack profiles

DDoS attack types have moved up the OSI network model over time, climbing from network to session, right up to today's application layer attacks. So what do they look like?

- **Volumetric:** consumes high bandwidth. The flood of incoming messages (high volume of data) to the target system forces it to shut down or slow service performance, thereby denying service to legitimate users.

- **Application layer:** consumes low bandwidth. Especially complex and difficult to detect, such attacks overwhelm specific elements of an application server infrastructure.

2.3 Common DDoS Attacks

Currently, there are a wide variety of attacks intended to overwhelm a target and make it inaccessible. Some of the most frequent attacks are:

- **TCP State-Exhaustion attacks:** These attempt to consume the connection state tables that are presented in many infrastructure components, such as load balancers or firewalls.
  - **SYN floods:** exploit the threeway handshake of the TCP setup – consuming enough server resources to make the system unresponsive to legitimate traffic.
  - **UDP & ICMP floods:** these are easy for attackers to generate since the UDP protocol doesn't validate source IP addresses, making them easy to forge. They flood random ports on a remote host with numerous UDP packets, causing the host to repeatedly check for the application listening at that port, and when no application is found reply with an ICMP Destination Unreachable packet. This process saps host resources and can ultimately lead to inaccessibility. Amplifying ICMP Echo Reply (pings) floods are also common. They overwhelm the target resource with ICMP Echo Request packets, generally sending pa ckets as fast as possible without waiting for replies.

- **DNS attacks:** DNS has become a favourite target for DDoS flooding attacks. Instead of taking down any web server by exhausting a DNS server, users simply cannot find their required website.

- **NTP attacks:** NTP is a networking protocol for clock synchronisation between computer systems. By sending a long reply to a short malicious request, the attacker is able to overwhelm a victim's system with UDP traffic. As the response is legitimate data coming from valid servers, it is especially difficult to detect.

- **Application attacks:**
  - **Slowloris attacks:** slowly deliver request headers forcing the webserver to keep connections open without completing the requests. This eventually overflows the maximum concurrent connection pool and leads to denial of additional connections from legitimate clients.
  - **SSL attacks:** by establishing numerous SSL sessions simultaneously, the application becomes unavailable because the system is engrossed with processing the previous requests.

03.
Why is an anti-DDoS solution important?

The volume, magnitude, type and complexity of DDoS attacks against organisations have increased substantially over time. Traditional security strategies such as firewalls, intrusion prevention systems (IPS) or web application firewalls (WAF) which only defend the perimeter of corporate communications, are no longer sufficient to protect an organisation's network. That's why it is no longer adequate to attempt to protect against these threats from an internal position. Today, an organisation requires an alliance with an ICT expert who can provide their business with robust protection against any kind of attack.

The number of companies attacked is increasing all the time and all industry sectors are vulnerable to DDoS, especially organisations whose business depends on the Internet. The Arbor Infrastructure Security Report 2014 identified a number of key trends, including:

- Shorter attack duration – almost 90% of attacks last less than an hour.
- Significant increase in the bandwidth consumed by DDoS attacks – approximately 20% of attacks detected are higher than 10 Gbps.
- Bigger packet-per-second attack volume – in the last year there has been a 389% increase in average attack bandwidth.
- Increase in the number of attacks – up by 22%.

Attack durations

In 2014, short and sharp attacks appeared to be more common, with 90 percent of attacks lasting less than one hour.

Attack frequency per month

The number of attacks experienced per month continues to increase year by year.

Application & infrastructure attacks

Infrastructure-layer attacks continue to dominate DDoS attacks but application-layer attacks have become increasingly common in recent years.

Demand for DDoS detection and mitigation services

Service providers are are seeing increased demand for DDoS detection and mitigation services.

Attack sizes

The size of DDoS attacks has increased dramatically. In 2014, attacks volume reached up to 300 Gbps.

Mobile network

Mobile devices began participating in DDoS attacks.

* Based on Arbor infrastructure security report (2014)

Given the growing number and scale of DDoS attacks, planning for their detection and mitigation is critical.

Many enterprises think it is unlikely their organisation will be attacked. However, in the 2015 PAC report, Incident Response Management, 67% of firms reported having had a cyber-breach in the last year, and 100% reported a breach at some time in the past*. This has occurred across companies from many industry sectors (financial services enterprises, e-commerce companies, government institutions, data centres, telcos, healthcare, retail companies, etc.) as they are all vulnerable to denial of service attacks, especially if their business relies on online operations.

The cost of downtime depends on several factors, such as the type of organisation, sector, number of people impacted, etc. What's more, the financial cost and impact on the business is staggering:

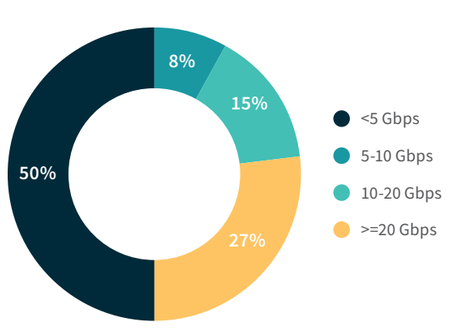
- Attacks against banks can interrupt their online services preventing customer and partner access to real-time resources or transaction processing.
- For online gambling companies, an outage of their services can lead to furious clients, complaints and lost revenues as well as brand and reputational damage due to the negative customer experience.
- The consequences for ISPs (Internet Service Providers) from a DDoS attack cannot be overstated. For example, if an attack targets their DNS infrastructure customers will not be able to reach a website or send an email. And when these business-critical applications are not available, operations and productivity simply cease.

DDoS attacks also continue to increase in complexity and have reached magnitudes of up to 300 Gbps. Furthermore, DDoS attackers are not only targeting the network layer (layer 3) but also the application layer (layer 7) where detection is far more difficult.

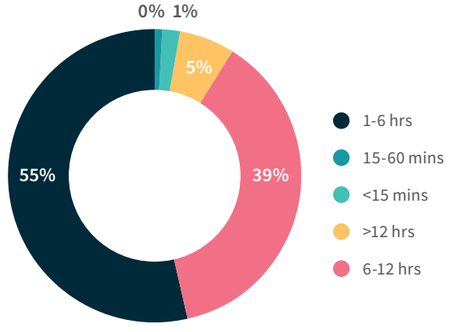
Clearly enterprises are at a higher risk of financial loss and reputational damage than ever before. Network security is now critical to their survival with DDoS Shield services offering the full protection and mitigation capacity necessary for corporate peace of mind.

* Source: Duncan Brown PAC Online – Incident Response Management, June 2015. How European Enterprises are Planning to Prepare for a Cyber Security Breach.

Mitigation by volume



Mitigation time



04. Towards a new world of protection

Because DDoS attacks are among the most difficult to defend against, it is essential to prepare a robust plan of action to ensure an immediate and appropriate response. This poses a huge challenge for all organisations.

Many enterprises rely on specific DDoS protection mechanisms that are not sufficient to stop complex, high capacity attacks before they reach the corporate network.

The problem is that some organisations are unaware of the scope and limitations of protection solutions or indeed the full scale and complexity of the current attacks. Hence they unwittingly run the risk of choosing the wrong technology for DDoS protection.

4.1 Why traditional tactics are not sufficient

Traditional security tactics are based on perimeter protection of the customer network. Devices such as Intrusion Prevention Systems (IPS) or firewalls, are essential elements of most security strategies, but they are simply not designed to stop modern DDoS attacks:

- They cannot stop attacks that are too large or complex.
- Attackers easily overrun perimeter devices by hitting it with more traffic than the upstream Internet connection or more traffic than the device can handle.
- HTTPS attacks will not be detected or mitigated.
- They have high CPU load, low throughput and performance.

It follows that traditional network security solutions such as firewalls, IPS and WAF are insufficient to handle the latest DDoS threats. Indeed they may actually exacerbate the problem by becoming bottlenecks during the attacks.

4.1.1 Firewalls

A common belief is that deploying a strong enough firewall will protect an organisation against DDoS attacks. Not so. The firewall alone is insufficient.

Firewalls offer a primary level of protection and are one of many options in a comprehensive toolkit when implementing an IT security policy. However, they were never intended to protect against DDoS attacks.

Initially, when attacks were simple they may have offered some protection. Unfortunately, the attacks are now far too large and complex to rely on this approach.

A firewall implements an access control policy between two or more security domains and inspects the traffic flow through each of them. It controls both incoming and outgoing network traffic and can allow certain packets to pass through or disable access for them. However, a firewall cannot evaluate the contents of 'legitimate' packets and can unknowingly let some attacks pass through onto the Web server.

Moreover, since firewalls are stateful, they are also vulnerable to DDoS attacks and often become the targets themselves. Examples of typical attacks affecting firewalls include syn flood, rst flood and fin flood.

4.1.2 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

An IDS monitors events in an IT system – complementing the first line of defence (behind firewalls). It offers some excellent attackdetection capabilities, but cannot mitigate the impact of the attacks and is not designed to withstand high-volume attacks.

An IPS identifies malicious activity and attempt to block it. However, it is not designed to stop the latest types of attacks. Similar to a firewall, an IPS is stateful and vulnerable to DDoS attacks.

An IPS looks for attack patterns inside connections as it inspects contents. It has a database of known vulnerabilities and compares the traffic with these vulnerabilities. IPS performance largely depends on the number of signatures it can manage.

An IPS is characterised by heuristic behaviour: it learns from the past at the expense of consuming large amounts of resources. This explains why an IPS is vulnerable to DDoS attacks that require complex analysis and, as a result, run out of memory session table or CPU, etc.

Examples of typical attacks affecting IPS include **slowloris, teardrop** and **tcp0window.**

4.1.3 Web Application Firewall (WAF)

A WAF controls the traffic that is delivered to a web server in order to protect it against security threats.

The mechanisms used by WAF devices affect memory and CPU. As a result, the number of servers that can be protected is usually rather small and only for at-risk URLs. The noncompromised URLs that are not protected subsequently become a target for DDoS attacks.

WAF devices are unable to detect floods of legitimate requests because they do not consider them to be malicious traffic. Hence such attacks easily exhaust the connection table.

Examples of typical attacks affecting WAF include **LOIC, Slowloris, RUDY** and **tcp syn.**

Defending against the current DDoS attacks that threaten a business's online availability requires a purposebuilt architecture that includes the ability to specifically detect and defeat increasingly sophisticated, complex and deceptive incursions. This approach relies as much onpreparation and response as it does on security intelligence, which informs strategy.

4.2 Challenges of the 'new world' of protection

The proliferation of DDoS attacks requires a new approach that provides complete DDoS protection to ensure business continuity.

In order to meet the demands of the 'new world' protection, a good DDoS protection solution should:

- Be delivered by an operator with strong skills in DDoS detection and mitigation.
- Have strong network bandwidth capabilities to be able to receive a huge amount of traffic without causing network congestion.
- Provide high mitigation capacity.
- Not add unnecessary latency to the networks that it protects.
- Ensure a quick response time.
- Protect all points of vulnerability – mitigating volumetric and application attacks as well as ISP neutrality.
- Possess built-in, cost-efficient scalability and flexibility.

4.3 Overview of anti-DDoS solutions

Some of the most popular DDoS responses, such as router filtering, black hole routing, local DDoS mitigation and over-provisioning of bandwidth, are not optimised to deal with increasingly sophisticated modern attacks.

4.3.1 Over-provisioning of bandwidth

This approach is commercially prohibitive as a DDoS prevention strategy and does not provide an efficient measurement, due to the continuous increase in volume of attacks. With current attacks capable of carrying up to 300 Gbps, even the best provisioned network can be overwhelmed. Furthermore, over-provisioning can address attacks at network-level, but not at application-level.

From an ISP (Internet Service Provider) perspective, the over-provisioning of bandwidth should be carried out with every interconnection point, i.e. with other ISP and peering connectivity, either nationally or internationally. In order to be effective, the overprovisioning should be completed as part of a purpose-built architecture against DDoS attacks, whose associated costs may be excessive when taken into consideration along with the trunk links.

From the point of view of a corporate customer, this solution would drive up the cost of the Internet connection and yet still not guarantee against application layer or very high volume attacks.

4.3.2 Router filtering

Many security teams use access control lists (ACLs) to filter out undesirable traffic as a strategy to defend their network. Although router ACLs can provide a first line of defence against basic and simple attacks, they are useless on their own against more sophisticated threats such as application level attacks.

Furthermore, the saturation of Internet interconnections is still not avoided.

This means that whilst router filtering could be a complementary solution for an ISP, it is never appropriate for a corporate customer.

4.3.3 Black hole routing

Black hole routing is when an ISP blocks all the traffic heading towards a victim from a domain or IP address. The problem with this is that it can result in not only discarding malicious traffic but also legitimate packets. Not only is the website in question affected but also any others that are sharing the same servers or even routers.

This means that black hole routing is not an ideal solution because it casts such a wide net – in some cases helping hackers to achieve the chaos they desire. Consequently, it should only be used in exceptional circumstances.

4.3.4 Local DDoS mitigation is not enough

Implementing a local DDoS solution has several limitations in the face of today's more sophisticated attacks:

- **It cannot stop DDoS attacks that are too large:** Although they have a greater chance of detecting suspicious traffic on the application layer, they can only protect their own bandwidth. It's unlikely that an enterprise, or even an ISP, would have enough bandwidth to manage the very large modern DDoS attacks. A local DDoS solution simply cannot manage volumetric network floods that saturate an enterprise's Internet pipe. Hence such attacks must be mitigated from the cloud.

ISPs should take into account that the dimensioning of their national interconnections is subject to peering agreements. So, despite having local equipment, it could still result in saturation of the links.

- **Limited knowledge of DDoS attacks and equipment:** Skilled network and security engineers are required to implement mitigation devices and a security strategy.

- **Commercial costs:** CAPEX on equipment is required. This can be expensive, have ongoing operational costs and indeed lie dormant until an attack is made.

Operating the service and acquiring experience in DDoS attacks mitigation is not easy. Finding skilled people and the learning process involved is quite difficult and time consuming. This means that even if you spend money on the acquisition of local equipment, you still need a strong, skilled team that understands how to apply the right countermeasures when an attack takes place.

Moreover, the cost associated with the Internet transit service also increases due to the associated expense of the malicious traffic which must be paid to the ISP.

4.3.5 Cloud solution with a connectivity provider (Tier-1)

A cloud-based solution provided by a Tier-1 ISP has significant benefits over other solutions. The service is completely transparent, both in configuration and operation, with no impact on customer routers.

The main characteristics are as follows:

- **Tier-1 network – global coverage:** The advantage of global visibility that comes from a Tier-1 network with strong experience in networks and routing.

- **High mitigation capacity:** The high mitigation capacity that this type of solution provides means that almost any kind of volumetric attack can be stopped.

- **Specialist team:** Mitigating DDoS attacks requires a large number of activities that are best managed by highly qualified operators, skilled in the service. Support is delivered by specific group exclusively devoted to dealing efficiently with DDoS attacks.

- **Transparent solution:** It is a non-intrusive solution which is completely transparent since the client's traffic is not inspected directly. When an attack is detected, only the IPs that are the target of the attack are diverted to the scrubbing centres. This means that clean traffic is delivered back to the network without affecting the rest of the services – assuring continuity of the services that are not under attack.

- **Full protection:** The service provides full protection with no need to hire DDoS protection from each ISP – as long as additional routing measures can be applied.

- **Cost savings:** This solution means no cost is incurred in relation to the traffic generated by the attack.

4.3.6 Cloud solution with a provider agnostic to the connectivity (No Tier-1)

Due consideration should be given to purchasing a carrier-agnostic service. However, when compared with a Tier-1 solution, the following should also be taken into account:

- **Carrier-agnostic service:** The solution is agnostic to the ISP, so if the client is connected to several ISPs, it is not necessary to purchase an anti-DDoS solution with each of them.

- **Global coverage:** The infrastructure is supported on several Tier-1 networks, so that the service has global coverage.

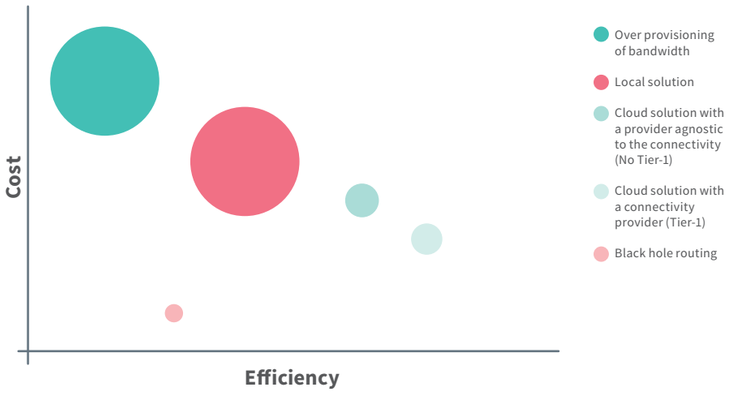
- **High cost:** These anti-DDoS service providers do not have their own network. As such they are required to pay their own Internet providers to transport the traffic to the scrubbing centres. As a result, the cost of this kind of solution is usually higher than a Tier-1 solution.

- **Higher latency:** Although the traffic is only diverted under attack, the solution diverts more traffic than necessary and adds latency for delivering the clean traffic. Additionally, the scrubbing centres are distributed internationally and many hops are added in order to divert the traffic towards them.

- **Clean traffic delivery:** The cleaning of malicious traffic is carried out by BGP diverting, while the clean traffic goes via GRE tunnel or a new physical link deployed between the scrubbing centre and the customer's router.

  On the one hand, delivery via GRE tunnel has a major impact on the CPU load because all C class traffic flows through the GRE tunnel, not just the IP traffic that is under attack. This means the customer's router must support GRE tunnels for delivering the clean traffic. The client must also possess powerful routers in order to re-inject the traffic. On the other hand, delivery through a new physical link to access the client network requires a new circuit to be installed. As a result, both a GRE tunnel and a scenario based on physical links means it will incur higher costs than a Tier-1 solution.

Comparison of anti-DDoS solutions



Size: Time taken to have the solution ready.
Colour: **Green** (no experience required).
Magenta (the stronger the colour, the more the experience required).

Comparison of Local vs Cloud solutions from an ISP perspective

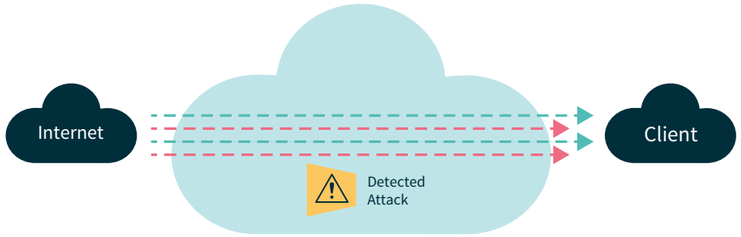
	Local solution	Cloud-based solution
Price	$$	$
Mitigation capacity	Low	High
Redundancy	Yes	Yes
Volumetric attacks detection	Yes	Yes
Application attacks detection	Not all	Not all
International mitigation	No	Yes
Defence against link saturation	No	Yes
Need to have security staff	Yes	No
Operational cost	Yes	No
CAPEX investment	Yes	No
Implementation time	Months	Days

05.
Our DDoS Shield solution

Our DDoS Shield service is an Internet transit value-added service, which offers a security solution that detects and mitigates DDoS attacks.

DDoS Shield represents an effective security solution that helps an organisation repel these attacks at our International network's entry points before they reach our customers' networks.

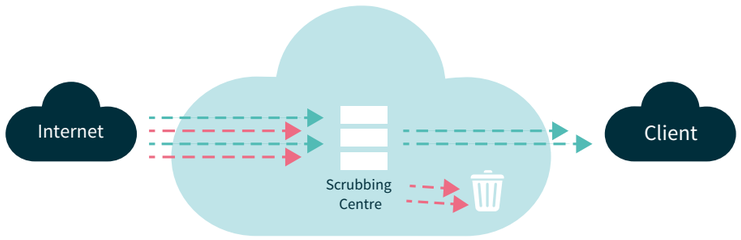
As a global telecommunications company, we provide customers with services that deliver maximum efficiency and a compressive protection against Internet threats. Our global Tier-1 network and strong experience in networks and routing allows us to combine all the required capabilities to provide a complete solution against DDoS attacks.



Detection

Legitimate traffic

Malicious traffic



Mitigation

5.1 Service description

The DDoS Shield service combines several functionalities, fully adapted to a customer's needs, to provide a highly effective solution against DDoS attacks:

- Monitoring.
- Detection.
- Mitigation.
- Traffic and attacks reporting.
- Real-time service status data via an online portal.

5.1.1 Monitoring

The system is capable of providing passive and non-intrusive monitoring of the network's traffic – analysing our international network backbone, gathering flow statistics from the border routers and providing global and perimeter detection of the entire network. This flexible service does not require the installation of equipment within the customer network, nor does it divert traffic when there is no attack or threat in progress.

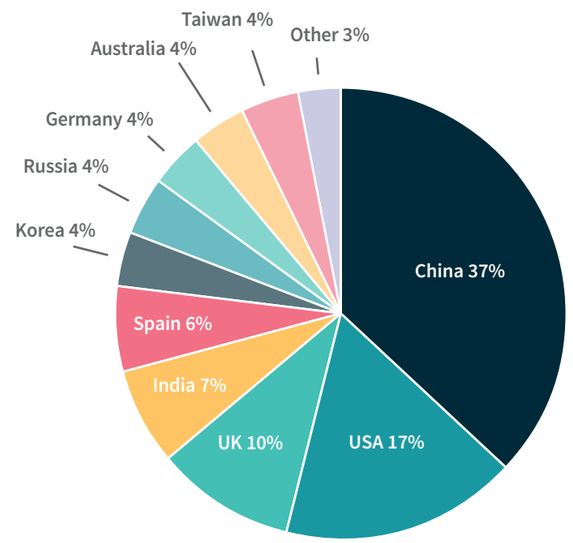
5.1.2 Detection

Using the monitored data, the service is able to detect any kind of volumetric attack targeted at a business at the entry point of our International Network.
Although many attacks have national origins, they usually make use of international networks in order to mask their real source. Attackers usually spoof the source IP address of the packets sent to a target in the hope of a third-party device sending unwanted data to the attacker's victim. This makes it difficult to block the attack as well as cloaking their real network location.

Our service provides global protection against such aggression. When abnormal traffic behaviour is detected, the service generates a warning that is stored and classified according to a specified threshold. It is then analysed by a team of professional technicians.

Top countries of origin

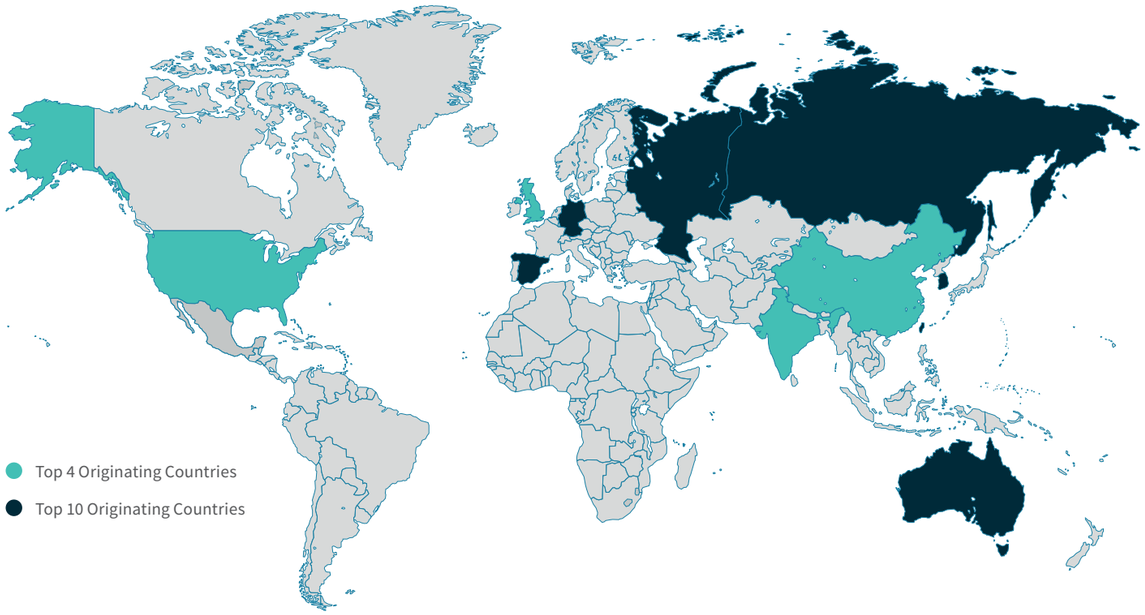
Fig.01*



* Source Fig.01 and Fig.02: Akamai: State of the Internet Report, September 2015. 2015 executive review [Q2 2015 connectivity & security]

Top sources of DDoS attacks in Q2 2015

Fig.02*



5.1.3 Mitigation

The DDoS Shield also deploys scrubbing centres installed in the network. Any traffic deemed suspicious by the detection equipment is then pushed towards these centres.

In the scrubbing centres the traffic is analysed and, if necessary, cleansed of malicious content. The system is able to identify both malicious and legitimate traffic. The former is discarded while the latter is re-directed to the client, ensuring service continuity.

With our DDoS solution only the targeted network's traffic is manipulated for mitigation. Furthermore, we implement different mitigation mechanisms.

The system is capable of mitigating an attack as close as possible to the entry point. Depending from where it enters the International Network, it will be sent to either one scrubbing centre or another without deviations to other remote Internet networks, so that low latency is guaranteed. Moreover, the service ensures that the clean traffic is delivered to clients in a transparent way, without affecting the rest of their services.

5.1.4 Customer on-premise equipment (CPE)

Customers have the option to implement on-premise equipment (CPE). CPE helps to protect against early application-layer attacks and is designed to detect and stop DDoS attacks immediately, without upfront configuration or any user interaction.

Additionally, CPE can be integrated with a cloud-based solution to mitigate attacks in the cloud. When an attack begins to saturate connection bandwidth, CPE appliance sends a signal to the cloud-based equipment and mitigation begins. In this way, our customers can maintain availability of networks, services and applications.

5.1.5 Local equipment operation or supply

If a customer has local security infrastructure and would like to use it to complement the cloud-based solution, we offer the options of operating the equipment or supplying it.

5.1.6 Attack reports

Once a DDoS attack is mitigated, the system provides a report containing data about the attack's volume, characteristics, evolution and any measures that have been taken. These reports include detailed information about attacks/anomalies, including graphs, protocols, entry and departure points, plus IP addresses targeted.

5.1.7 Traffic reports DDoS mitigation is not enough

The service can also generate customised reports related to traffic, regardless of DDoS attacks, including:

- Statistics on traffic volume broken down by application.
- Statistics of IP sub network distribution or autonomous systems (ASN) towards which most traffic is sent or received.
- A view of the traffic on a network, country by country, etc. Such reports provide additional value by giving tangible results which show exactly how the service is running and protecting a network.

5.1.8 Client Portal

The service also provides customers with an online portal where it is possible to consult a wide range of data and information. The portal gives full visibility of the following:

- **Service:** provisioned IP address.
- **Attacks and mitigation actions:** access to attack reports.
- **Traffic:** access to traffic reports.
- **Alarms:** Information about alarms in progress, recent alarms (those that have been set off in the last 24 hours), classification of the alarm/ anomaly according to their degree of potential impact or severity (high, medium or low).

More information about our service can be found on Page 16.

Our DDoS Shield value proposition

We combine all the capabilities of our platform to provide a smart and global service that fully protects customers from DDoS attacks whilst minimising impact on their business operations.

Complete Managed Cloud Service

Our DDoS Shield service is a managed cloud-based service. Solutions based on the cloud such as the one we offer, provide scalability and a global solution in order to protect your business against the most common types of DDoS attacks.

We are able to mitigate an attack as close as possible to the source in order to prevent your Internet links from becoming saturated.

In addition, we can handle larger attacks than any single organisation with an on-premise solution. Local solutions can be swamped by attacks that are higher than the local mitigation capacity. They overwhelm the international links and degrade the Internet transit service – not just impacting on the intended target victim but also on the victim's customers.

Moreover, our DDoS Shield service is able to cover a huge number of connectivity scenarios using several mechanisms that simplify problem resolution for our clients.

Wide coverage

Our Tier-1 international network is interconnected with the leading Internet players and provides daily traffic of more than 4.5 Tbps. The DDoS Shield service provides global visibility covering our entire international network.

The solution protects the customer's network from the outside and monetises the economic damages caused not only to them but also to their own customers.

Strong experience

We combine all the capabilities of our global Tier-1 network and strong experience in networks and routing as a leading ISP. The result is a complete service that we believe no other set of solutions can match.

24/7 support

Telefonica is ISO/IEC 27001:2007 certified and is a member of FIRST, the global Forum for Incident Response and Security Teams. As an organisation we have over 7 years' experience in this space, and our team consists of highly qualified and knowledgeable security professionals.

So that our customers do not have to invest in highly skilled, around-theclock personnel to operate the service efficiently, we offer 24/7 worldwide support to fight DDoS attacks. Our expert technicians constantly monitor, detect and analyse the real-time evolution of attacks – responding instantly to malicious traffic. As a result, we are able to mitigate attacks within minutes, having routed the malicious traffic through our scrubbing centres.

Smarter and reliable

We use proprietary, market-leading technology to detect and route all the suspicious traffic to the nearest scrubbing centre in our global network. Several detection and scrubbing centres are deployed in our international network to deliver a reliable and widely available solution capable of mitigating attacks close to their entry point.

Granularity and transparency

We are able to proactively detect and route all the suspicious traffic to the scrubbing centre, mitigating the attacks before they reach an organisation's network.

The deviation of the suspicious traffic to the scrubbing centres is based on specific IP announcements so that only the IPs attacked are diverted. The clean traffic is simply delivered back to our customer's network without affecting the rest of their services.

Low Latency

The scrubbing centres are situated in our own network. This means we deal with the attacks as close as possible to their source. The traffic is diverted as little as possible in order to guarantee that our latency is always lower than that of other solutions in the market.

Privacy

The service provides passive and non-intrusive monitoring of the customer traffic since the traffic is not directly inspected. It analyses statistical information on traffic which guarantees the privacy of the packets.

Flexible and versatile

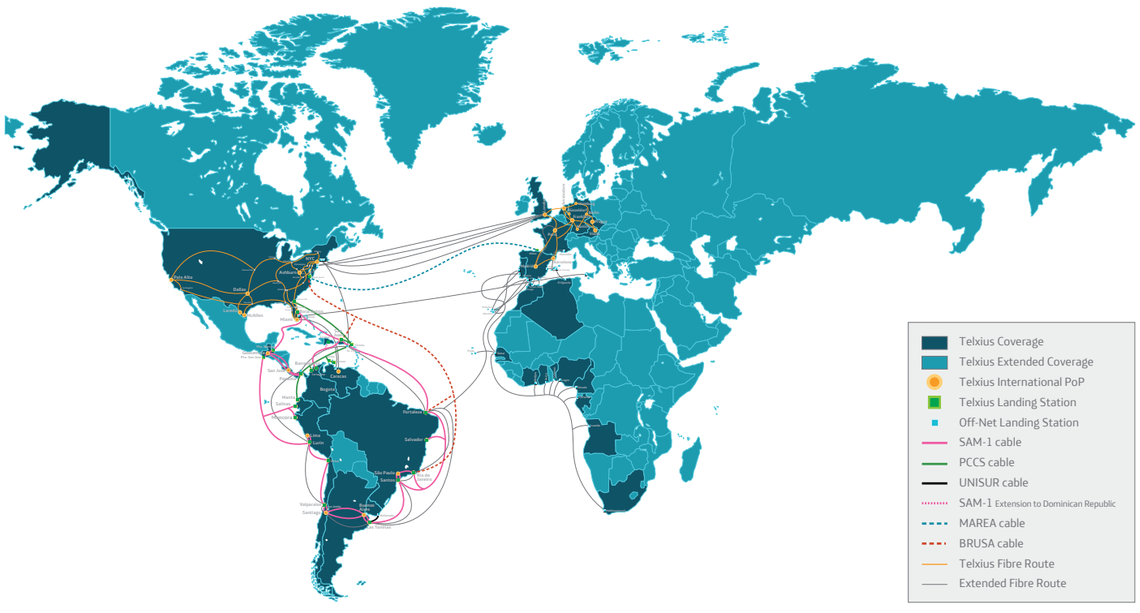
The versatility of our service means that our solution can meet each customer's individual needs. It's totally adaptable to any connectivity and flexibility required through contract options.

Quality of service commitment

We are committed to guaranteeing specific Service Level Agreements (SLA) for the Global DDoS Shield Service:

- Time information after an attack detection SLA.
- Time for starting a mitigation SLA.
- Availability of the service SLA.

Telxius International Network



DDoS Shield

Global visibility of a Tier-1 network	With a capacity higher than Tbps
Full protection of your network	Global visib Detection and mitigation of any kind of attack: network, transport and application layers ility of a Tier-1 network
Maximum capacity	Higher mitigation capacity than other solutions in the market
Experience	Expertise in DDoS detection and mitigation backed up by 7 years operating the service
Service adapted to your needs	Flexible, versatile and adaptable
Global service	24x7 worldwide support provided by a team of security experts staff

Why Telxius?

Telxius, created in 2016, is the new global telecommunications infrastructure company of the Telefónica Group, whose aim is to capture the exponential increase of data traffic expected in the coming years. With an international high-capacity cable network, Telxius manages a 65,000 km network of submarine fiber optic cables connecting Europe and America, 31,000 km of which are owned by Telxius. It includes, among other infrastructures, SAM-1, the submarine cable system which has connected the United States with Central America and South America since the year 2000, PCCS (Pacific Caribbean Cable System), which connects the US, Puerto Rico, Curazao, Colombia, Panama and Ecuador, and Unisur, which connects Uruguay and Argentina. It is expected that BRUSA, the new offshore cable measuring nearly 11,000 km and connecting Brazil, Puerto Rico and the US, will be operational in 2018, as well as MAREA, a cable which will link the United States and Europe, in partnership with Microsoft and Facebook. Telxius also features 16,000 telecommunications towers in five countries, with one of the largest tower catalogues in the market among independent infrastructure companies.

TELXIUS

Enabling Communication

Find out more about our services and the benefits they can bring to your business, visit: **telxius.com** or email us at: **sales@telxius.com**