KASPERSKY DDOS PROTECTION

Discover how Kaspersky Lab defends businesses against DDoS attacks

CYBERCRIMINALS ARE TARGETING BUSINESSES

If your business has ever suffered a Distributed Denial of Service (DDoS) attack, you'll already know that the financial and reputational costs can be devastating. However, even if your business has been lucky enough to escape the attentions of the cybercriminals and hackers that launch these attacks, the outlook for the future may not be so positive.

THE VOLUME AND SEVERITY OF ATTACKS IS INCREASING

Unfortunately, in recent years, the cost of launching a DDoS attack has fallen significantly – and that means more attacks are being initiated than ever before. At the same time, today's attacks are more complex and they're at a scale that can overwhelm the target business's communications bandwidth in just a few seconds – almost instantly debilitating vital, internal business processes and totally disabling the victim business's online presence.

With all sizes of business relying on their IT infrastructure and website to underpin almost all of their mission-critical processes, extended downtime – that can result from a DDoS attack – is not an option. Clearly, with the volume, scale and severity of modern attacks, it's no longer viable for any business to put off any thoughts of DDoS protection and mitigation until the point at which their infrastructure is already under attack. Instead, businesses – and public sector organizations – need to be aware of the threats and ensure they have adequate DDoS defense measures in place.

'FOREWARNED IS FOREARMED'

Every business needs to have an anti-DDoS strategy – ready to 'go live' as soon as an attack is detected. Then, in the event of an attack, the business will be able to mitigate the effects – without delay – in order to:

- Minimize downtime for business-critical infrastructure & processes
- Ensure customers can continue to access online services
- Maintain productivity for employees
- Minimize reputational damage

DDOS ATTACK METHODS

Cybercriminals and hackers are using a number of different techniques to implement DDoS attacks that disable or overload the target business's IT infrastructure.

VOLUMETRIC ATTACKS

These attacks are increasingly common. By generating traffic levels that exceed the target business's available bandwidth, the attack saturates the capacity of the victim's corporate Internet connection – and that disables or delays all online activities.

APPLICATION LAYER ATTACKS

Application layer attacks try to crash the servers that are running vital applications – such as the web servers that the victim's online presence depends on.

OTHER INFRASTRUCTURE ATTACKS

Attacks that aim to disable network equipment and / or server operating systems can totally halt the operation of key business processes.

HYBRID ATTACKS

Cybercriminals also launch complex attacks that combine several methods – including volumetric, application layer and infrastructure attack techniques.

THE TOTAL DEFENSE AND MITIGATION SOLUTION

Kaspersky DDoS Protection delivers a total, integrated DDoS attack protection and mitigation solution that takes care of every stage that's necessary to defend your business. From continuous analysis of all of your online traffic, through to alerting you about the possible presence of an attack and then receiving your redirected traffic, cleaning your traffic and returning 'clean' traffic to you, Kaspersky DDoS Protection provides everything your business needs to defend against – and mitigate the effects of – all types of DDoS attacks.

KASPERSKY DDOS PROTECTION INCLUDES:

- Kaspersky Lab sensor software – that runs within your IT infrastructure
- The services of our global network of data traffic 'cleaning centers'
- Support from our Security Operations Center and DDoS protection experts
- Detailed, post-attack analysis and reports

HOW KASPERSKY DDOS PROTECTION WORKS

Kaspersky Lab's sensor software collects information about all of your communications traffic – 24x7x365. The sensor is installed as close as possible to the resource that you wish to protect – and it continuously gathers data about your traffic, including:

- Header data
- Protocol types
- Number of bytes sent and received
- Number of packets sent and received
- Activities and behavior – of every visitor to your website
- All metadata about your traffic

All of this information is sent to Kaspersky Lab's cloud-based servers, where it is analyzed so that we can build up profiles of how typical visitors behave and profiles of your typical traffic – and how that traffic can vary according to the time of day and the day of the week, plus how special events can affect your traffic patterns. With this detailed understanding of your 'normal traffic conditions' and 'normal visitor behaviors', our cloud-based servers can accurately assess your live traffic conditions – in real time – and rapidly identify anomalies that can indicate that an attack has been launched against your business.

In addition, our threat intelligence experts continuously monitor the DDoS threat landscape – in order to identify new attacks. This specialist intelligence helps to ensure Kaspersky Lab customers benefit from a rapid response to the launch of an attack.

AVOIDING FALSE ALARMS… THEN CLEANING YOUR TRAFFIC

As soon as a possible attack against your business is identified by our servers or our intelligence experts, Kaspersky Lab's Security Operations Center will receive an alert. To help avoid false alarms – and unnecessary disruptions for your business – Kaspersky Lab engineers check to confirm that the traffic anomaly or suspicious behavior has resulted from a DDoS attack. Then, our engineers immediately contact your business – to recommend that your traffic is redirected to our network of cleaning centers.

During the attack, with all of your traffic now passing through one of our cleaning centers:

- Your infrastructure is no longer being overwhelmed by the sheer volume of 'junk traffic'
- Our cleaning process discards all junk traffic
- Legitimate traffic is delivered back to you – from our network of cleaning centers

… and the entire process is totally transparent to your employees and customers.

SETTING UP PROTECTION IS QUICK AND EASY

When you choose Kaspersky DDoS Protection, there's a small number of set up tasks before your 24x7 monitoring – and your 'live attack' communications channels – are established. Kaspersky Lab – and its partners – can take care of as much or as little of the set up process as you require.

If you require a turnkey solution, Kaspersky Lab and its partners can cover the vast majority of set up procedures – including:

- Installing the sensor software and hardware on your site
- Setting up traffic redirection to our cleaning centers
- Setting up 'clean' traffic delivery to your business

… then, all you'll need to provide is a separate Internet channel to the sensor – so that Kaspersky DDoS Protection can continue to collect data when your main Internet channel has been disabled by an attack.

THE SENSOR – ENABLING 24X7 MONITORING

Kaspersky Lab's sensor software is supplied complete with a standard Ubuntu Linux operating system. Because the sensor software runs on a standard x86 server – or on a virtual machine* – there's no special hardware for you to maintain.

Because the sensor is connected to the SPAN (Switched Port Analyzer) port, it's able to get the best possible view of all traffic that's flowing into and out of the resource that it's protecting.

As soon as the sensor is connected to your infrastructure, it starts collecting data on your incoming and outgoing traffic. It analyses each packet's headers and sends information to the Kaspersky DDoS Protection cloud servers – where we build statistical profiles of 'normal traffic behavior' and 'normal visitor behavior' for your business.

In order to maintain privacy for your communications – and help with your compliance commitments – the sensor does not capture the content of any of the messages within your communications traffic. The sensor only gathers data about your traffic – so the confidentiality of your messages is never compromised by any of Kaspersky DDoS Protection's processes.

*The virtual machine must meet or exceed the minimum performance requirements specified by Kaspersky Lab.

TRAFFIC REDIRECTION

During normal conditions – while the cloud-based Kaspersky DDoS Protection servers are monitoring for any signs of a DDoS attack – your traffic is delivered directly to your corporate network. Your traffic is only redirected – to our global network of cleaning centers – after an attack has been detected and your business has confirmed that it wishes to redirect its traffic.

Kaspersky DDoS Protection gives you a choice of redirection methods:

- Border Gateway Protocol (BGP)
- Domain Name System (DNS)

GENERIC ROUTING ENCAPSULATION (GRE) VIRTUAL TUNNELS

Whichever redirection method is best for your business, GRE virtual tunnels are used to enable communication between your border gateway – or router – and each relevant Kaspersky DDoS Protection cleaning center.

In the event of a DDoS attack being launched against your business, all of your traffic can be rerouted to one of our cleaning centers. The GRE virtual tunnels are then used to deliver the cleaned traffic – from our cleaning centers, to your business.

CHOOSING BETWEEN BGP AND DNS

Whether you set up your traffic redirection via BGP or DNS, will largely depend on the nature of your corporate IT and communications infrastructure:

- For BGP, you'll need to have:
  - A provider-independent network – that includes the resources that you wish to protect
  - An autonomous system

  … and most large businesses are able to meet these criteria.
- For DNS, you'll need to be able to:
  - Manage your own domain zone for the resources that you're looking to protect
  - Set the Time to Live (TTL) for DNS records to 5 minutes

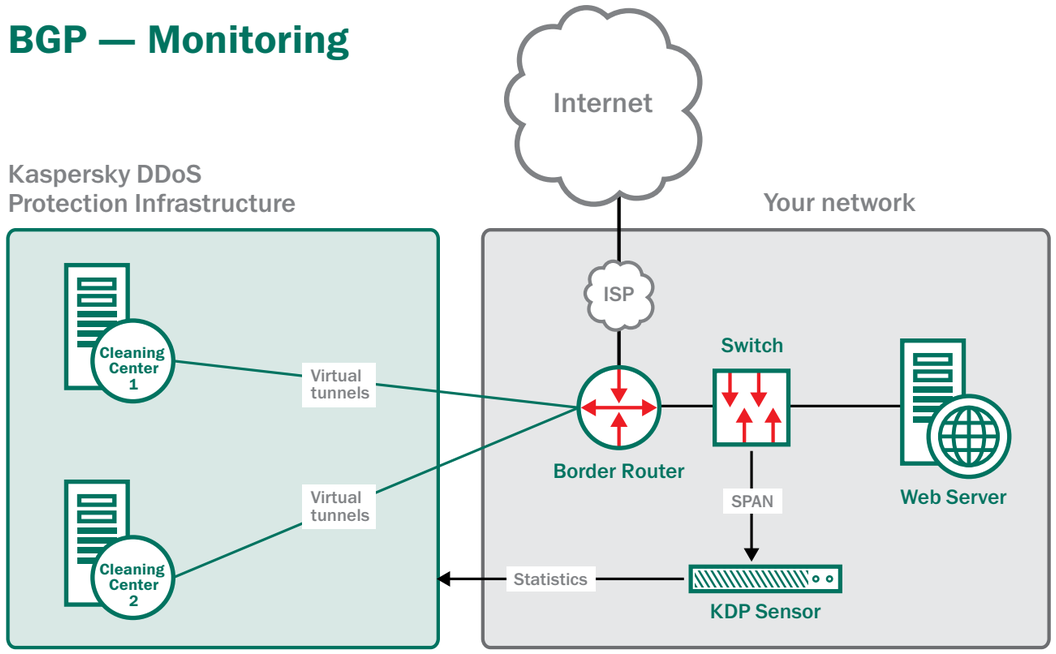
Generally, during an attack, the BGP method achieves faster redirection of traffic – so BGP is often the preferred method for most businesses.

▶ HOW BGP REDIRECTION WORKS

MONITORING

In monitoring mode, all of your traffic is delivered directly to your business. However, the GRE virtual tunnels are in 'live' operation – with your routers and our BGP routers frequently exchanging status information… so the Kaspersky DDoS Protection cleaning centers are ready to receive your redirected traffic whenever necessary.

BGP — Monitoring

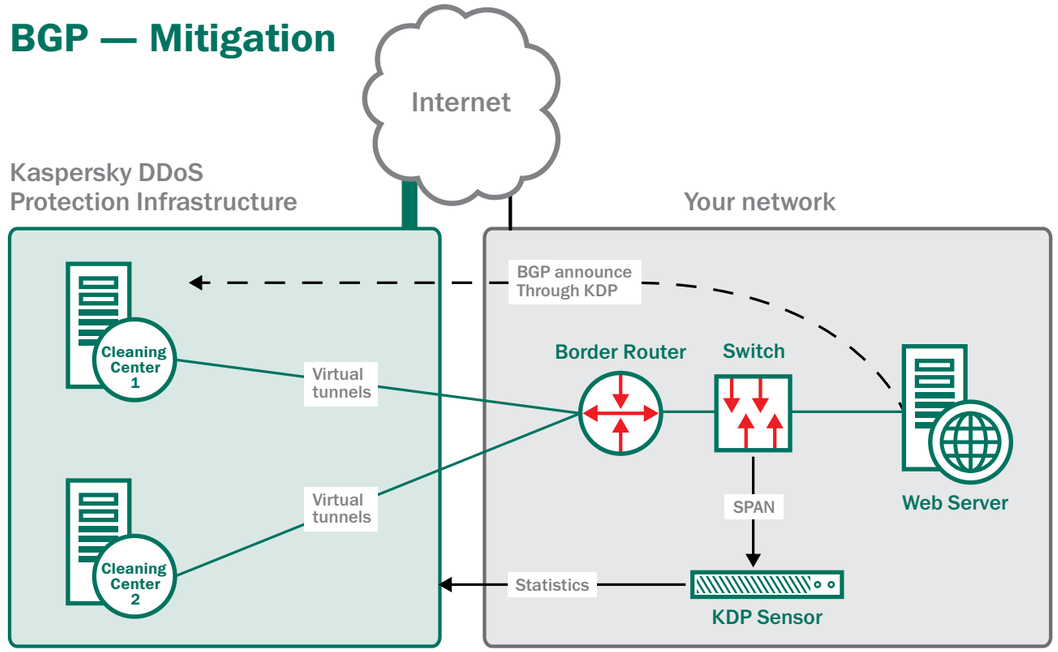


DURING AN ATTACK

When a traffic anomaly is identified by Kaspersky Lab's sensor – and the start of an attack is confirmed by Kaspersky Lab's engineers – you can choose to redirect all of your traffic to a Kaspersky DDoS Protection cleaning center.

Throughout the attack, the Kaspersky Lab sensor will continue to gather information and send it for analysis by the cloud-based Kaspersky DDoS Protection servers.

BGP — Mitigation



AFTER AN ATTACK

When the attack has ceased, your traffic is once more sent direct to your business. The sensor continues to gather data about your traffic – and constantly passes this data to our cloud-based servers, so that we can continuously refine our behavior profiles for your normal traffic conditions.

The virtual tunnels remain live – exchanging status information between your routers and Kaspersky Lab's routers – so that Kaspersky DDoS Protection is ready to act if another attack is launched against your business and you choose to redirect your traffic again.

Kaspersky Lab's experts will also provide you with detailed, post-attack analysis and reporting on exactly:

- What happened during the attack
- How long the attack lasted
- How Kaspersky DDoS Protection dealt with the attack

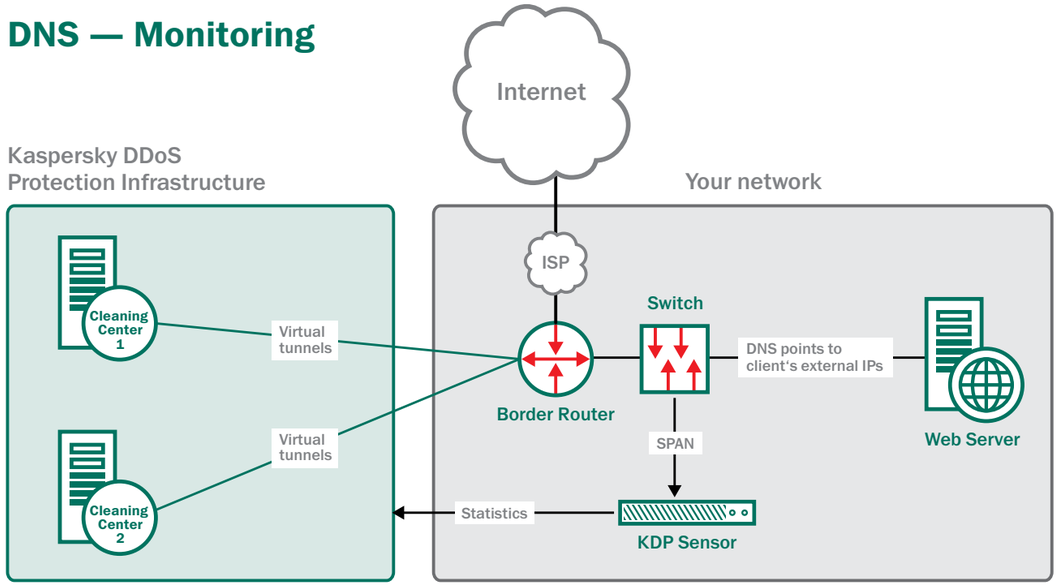
▶ HOW DNS REDIRECTION WORKS

MONITORING

During initial set up, Kaspersky Lab allocates one of its pool of Kaspersky DDoS Protection IP addresses to your business. This address will be used in the event of an attack.

In monitoring mode, all of your traffic is delivered directly to your business – via its normal IP address / addresses. However, the GRE virtual tunnels are in 'live' operation – with your routers and our BGP routers frequently exchanging status information… so the Kaspersky DDoS Protection cleaning centers are ready to receive your redirected traffic whenever necessary.

DNS — Monitoring

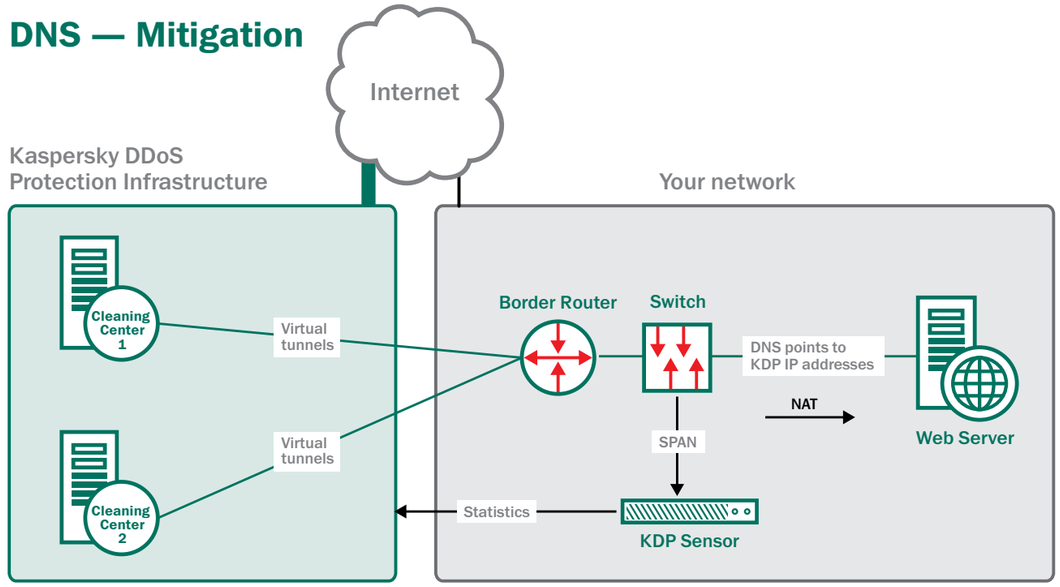


DURING AN ATTACK

When a traffic anomaly is identified by Kaspersky Lab's sensor – and the start of an attack is confirmed by Kaspersky Lab's engineers – you simply change your business's IP address in the DNS A record… so that your business is now using the Kaspersky DDoS Protection IP address that was allocated to you during initial set up. At the same time, because hackers can directly attack your IP address, your ISP must block all traffic to your original IP address – with the exception of communications with Kaspersky Lab's DDoS Protection infrastructure.

Having changed your IP address, all your traffic is redirected to Kaspersky Lab's cleaning centers. 'Clean' traffic is then delivered back to your business – from our cleaning centers – via the GRE virtual tunnels.

DNS — Mitigation



AFTER AN ATTACK

When the attack has ceased, you can unblock your original IP address and change the DNS A record – so that your traffic is once more sent direct to your business.

The Kaspersky Lab sensor continues to gather data about your traffic – and constantly passes this data to our cloud-based servers, so that we can continuously refine our behavior profiles for your normal traffic conditions.

The virtual tunnels remain live – exchanging status information between your routers and Kaspersky Lab's routers – so that Kaspersky DDoS Protection is ready to act if another attack is launched against your business and you choose to redirect your traffic again.

Kaspersky Lab's experts will also provide you with detailed, post-attack analysis and reporting on exactly:

- What happened during the attack
- How long the attack lasted
- How Kaspersky DDoS Protection dealt with the attack

THREAT INTELLIGENCE – FOR EVEN BETTER DEFENSE

There is another important defense component within Kaspersky DDoS Protection – and it's a component that other vendors cannot match.

Kaspersky Lab is the first anti-malware vendor to provide a DDoS protection solution – and that means no other anti-DDoS supplier can match the expertise and scale of our in-house security intelligence department and infrastructure.

As part of their work on cutting-edge IT security, our threat intelligence experts continuously monitor the threat landscape – to identify new malware and emerging Internet threats. The same experts – and the same sophisticated methods – are also used to monitor the DDoS threat landscape. This specialist intelligence helps us to achieve earlier detection of DDoS attacks… so your business can benefit from more rapid protection.

MULTI-LAYERED PROTECTION

With a unique combination of continuous traffic monitoring, statistical analysis and behavior analysis – plus our specialist, proactive DDoS attack intelligence – we deliver a more rigorous DDoS protection solution.

DataSheet_DDoS/August14/Global

KASPERSKY lab