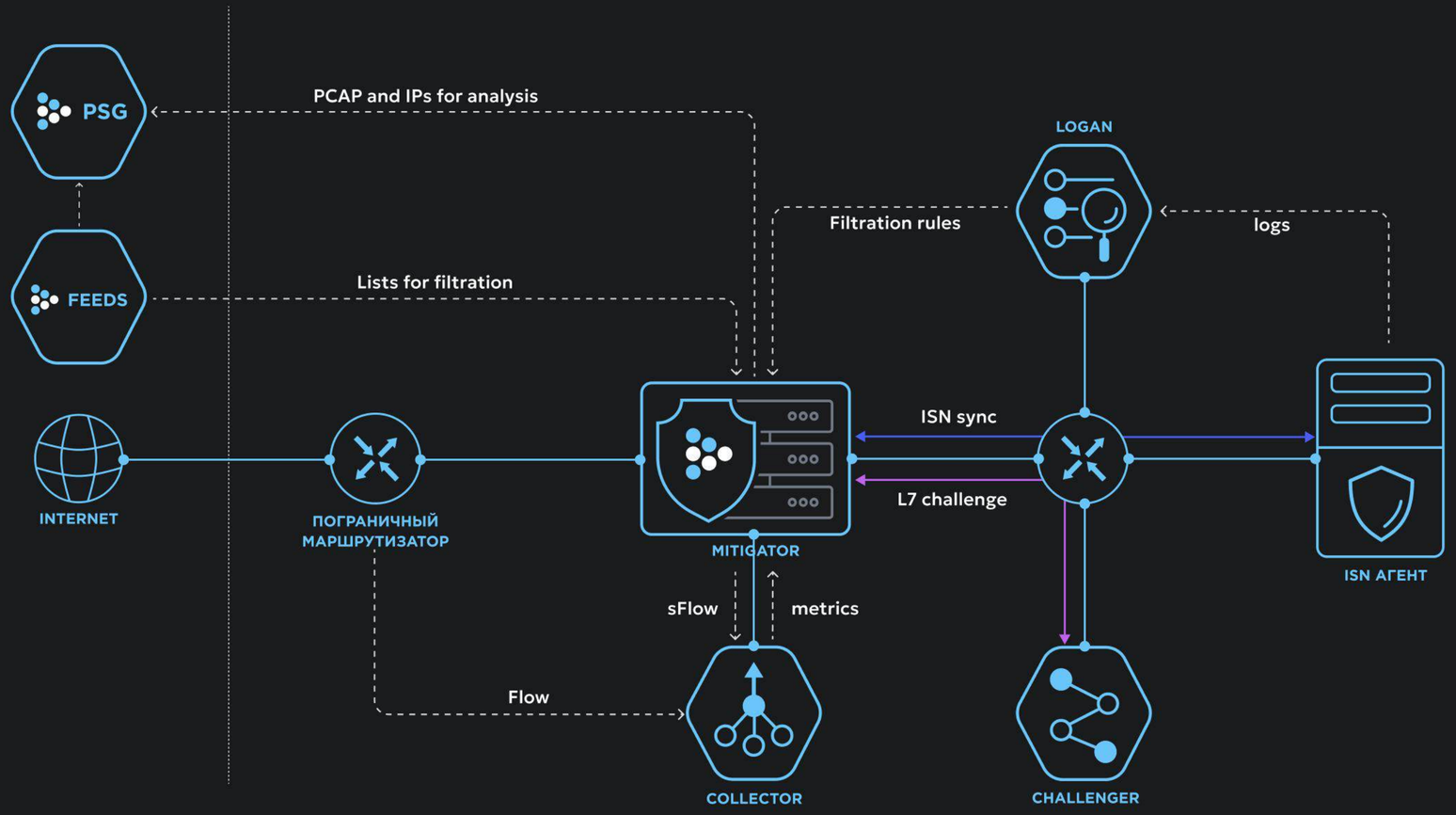
MITIGATOR

DDOS PROTECTION

Key features

Ecosystem



MITIGATOR is not limited to just traffic scrubbing, it is an entire ecosystem, which also includes:

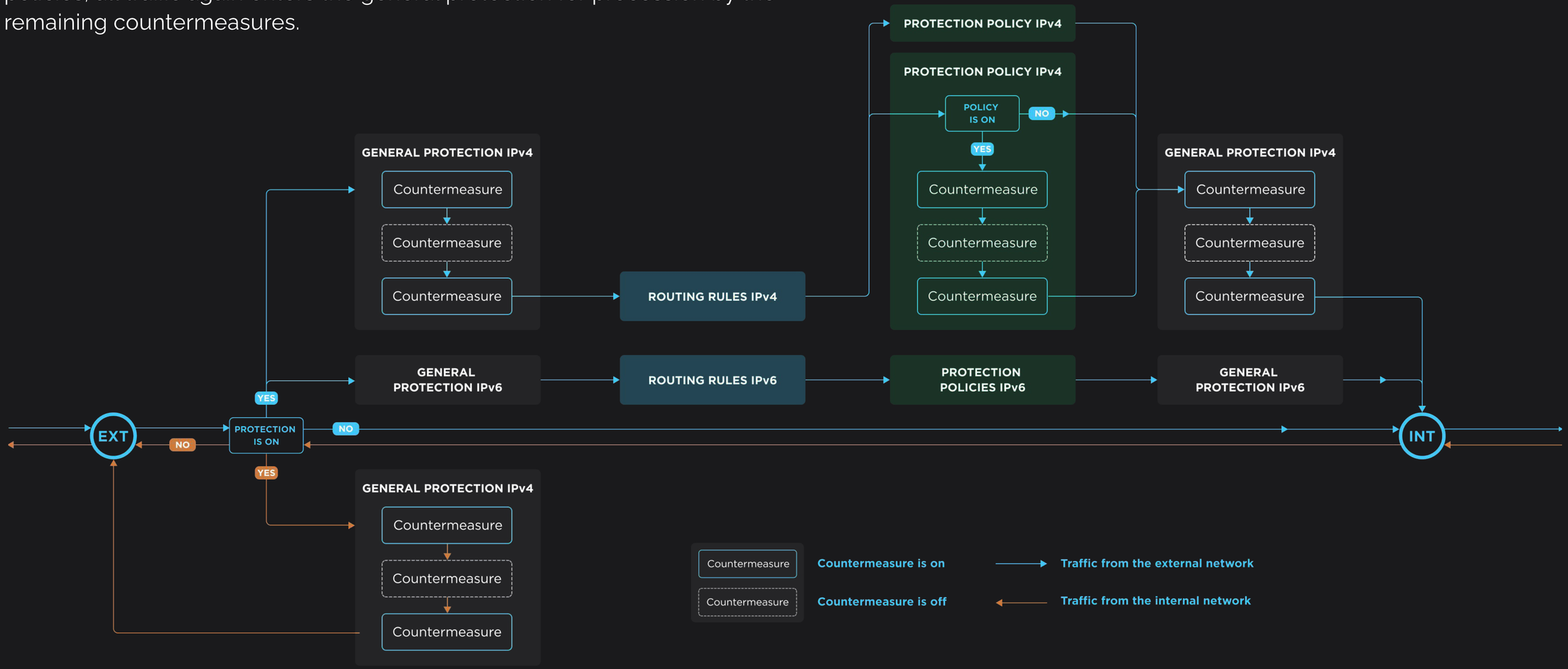
- Collector - for collection and analysis of network equipment telemetry.
- Logan - for protection of the Web using log analysis.
- Web-Challenger - for authentication of senders using the challenge-response method within HTTPS.
- ISN-агент - which allows countermeasures to work in an asymmetric traffic mode while being invisible to the user.
- Feeds - reputation lists of IP addresses, autonomous systems and TLS fingerprints.
- PSG - a network traffic dump analysis service designed to identify patterns. Additionally, the service analyzes IP address lists and TLS fingerprints.
- bpf.mitigator.ru - for compilation and validation of programs for BPF.
- Cloud - a comprehensive protection service for corporate clients.
- and more.

MITIGATOR DDOS PROTECTION

Cascade countermeasures application

All traffic coming from the external network is first processed by global countermeasures of general protection. After passing the global countermeasures, the traffic is distributed to different protection policies, where it is processed according to individual policy settings. After exiting policies, all traffic again enters the general protection for procession by the remaining countermeasures.

MITIGATOR can process traffic from the internal network in the general protection, which allows usage of bidirectional and high-performance stateless firewall with a large set of rules.



MITIGATOR DDOS PROTECTION

Flexible traffic distribution over protection policies

MITIGATOR allows traffic separation and filtering not only by the destination address, but by any combination of 5-tuple as well. Thus, specific services' traffic can be diverted to separate protection policies and only necessary countermeasures can be applied for scrubbing

Hardware bypass support

MITIGATOR supports network adapters that use hardware bypass. In case of system or hardware platform failure, the network adapter switches to bypass mode at the physical layer. Traffic is redirected from port to port, bypassing the network adapter controller.

Wide network integration capabilities

MITIGATOR can operate in L2-transparent and L3-router, inline, on-a-stick and common lan modes. The deployment method depends on the network structure and tasks. Traffic to MITIGATOR can be directed constantly or only at the time of an attack.

Cluster Operation

MITIGATOR supports cluster operation, which ensures maximum protection reliability due to redundancy. Traffic procession performance increases due to the growth in the number of filtering nodes. Data synchronization mechanisms between cluster instances ensure seamless traffic transition.

Docker

The MITIGATOR software is supplied as a set of Docker containers. To update the system version, only few commands are required

Works on common hardware

MITIGATOR supports a wide range of x86-64 processors and network cards

Service Creation and Access Sharing

MITIGATOR can be used to create a DDoS protection service. Traffic separation allows the provision of independent filtering settings for individual clients. Flexible role model and password management policy available.

Autodetection

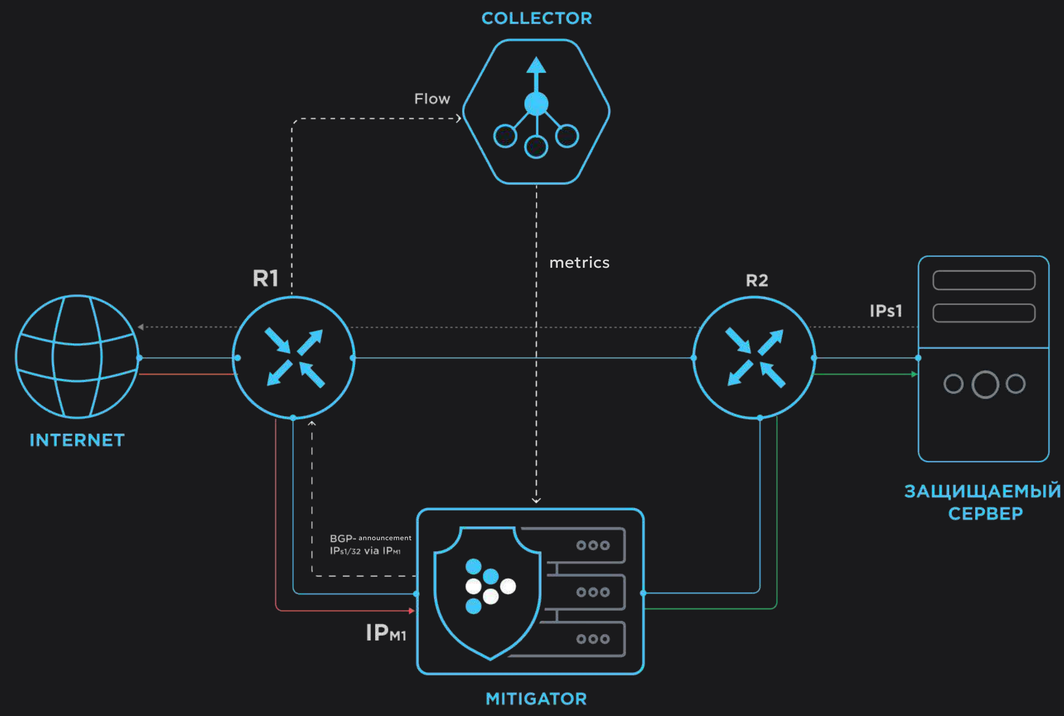
MITIGATOR has a built-in function for automatic activation and deactivation of mechanisms based on set thresholds, both for traffic passing through the system and for data from the Flow collector. Independent setup of thresholds and response time on them being crossed is supported for each protection policy

Soft start and soft stop

MITIGATOR supports an operating mode in which active countermeasures do not drop traffic from unknown connections and records about them are added to the tables of authenticated connections for a set time after their activation. Thus, the traffic of the connections established before the protection was enabled, is not affected. When disabled in the Soft Stop mode, MITIGATOR will not break established sessions, but will wait for them to close

Flow collectors support

Allows the detection of attacks and activation of protection for individual policies without constant direction of traffic to MITIGATOR, as well as collection and visualization of statistical information in various sections, both in real time and historically

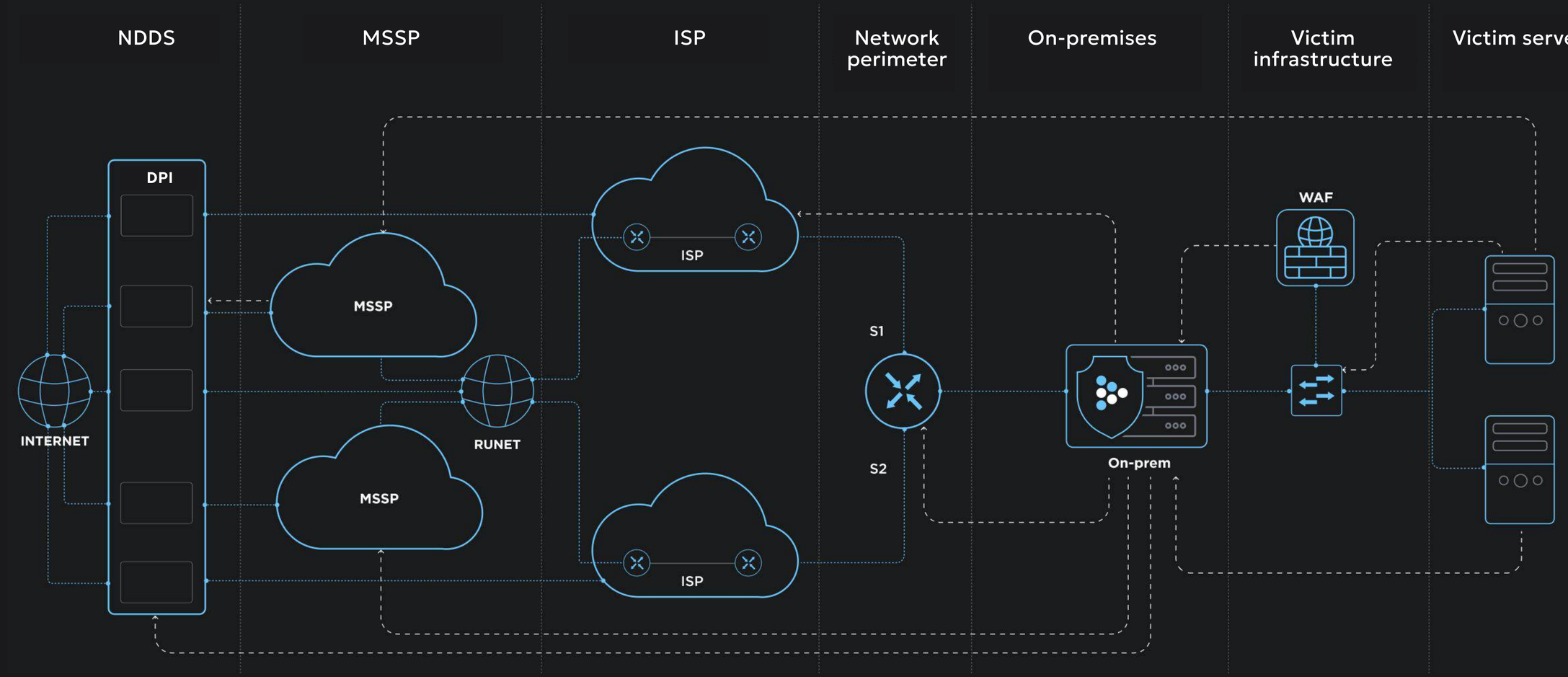


MITIGATOR DDOS PROTECTION

Layered protection

MITIGATOR can signal upstream telecom operators and security service providers about an attack and automatically activate filtering at higher layers.

REST API and named lists functionality allows for the integration of external systems with MITIGATOR in order to load IP addresses for filtering. Cloud signaling with DDoS protection solutions from well-known vendors is also supported.



MITIGATOR DDOS PROTECTION

BGP and BGP FlowSpec

Supports interaction via BGP and BGP FlowSpec to redirect traffic to scrubbing, signal upstream equipment, and make blackhole announcements. Each MITIGATOR instance is an independent BGP speaker with the ability to automatically remove announcements if the filtering device fails.

GRE

MITIGATOR supports two scenarios of interaction with GRE tunnels: delivery of scrubbed traffic to the protected service, and reception of traffic from a third-party service for subsequent scrubbing

Named Lists

While specific IP addresses or TLS fingerprints can be set up, MITIGATOR allows for usage of named lists from various sources, including MITIGATOR Feeds - regularly updated reputation lists of IP addresses, ASes, and JA3 fingerprints created by the MITIGATOR team

Test mode

MITIGATOR has a built-in non-traffic-affecting testing mechanism for the security settings. Test mode can be activated for individual countermeasures or the entire policy

Host protection

The host protection detector and host activation mechanism allows application of checks only to IP addresses whose traffic exceeds a set threshold. This enables flexible configuration of traffic processing and makes no impact on the traffic of unattacked services

TCP protection for Traffic Symmetry

MITIGATOR supports SYN-proxy (TCP Splicing) protection if outgoing traffic from protected resources passes through it

TCP protection for Traffic Asymmetry

To protect against TCP attacks while only incoming traffic is present, MITIGATOR uses widely accepted checking methods by resetting the TCP session and using the wrong sequence number with different combinations of flags.

In addition to the standard protection mechanisms, a unique mode of operation with ISN synchronization is available, in which protection against traffic asymmetry does not require unnecessary packet exchange or disconnection with the client.

Host protection can be activated only for the servers under attack, which eliminates the negative impact on the traffic of other services

WAF integration

It is possible to send traffic of the protected service for analysis and additional checks to Web Application Firewall. Redirection parameters are set individually for each protection policy

REST API

REST API allows you to integrate with other security and monitoring systems and perform any actions in MITIGATOR with their assistance and to automate management

HTTPS protection with and without decryption

MITIGATOR can protect Web applications without traffic decryption via different TLS parameters analysis methods and usage of JA3/JA4 fingerprints. In combination with other countermeasures and a Web server log analyzer, it is possible to achieve maximum protection efficiency without traffic decryption.

In addition, senders can be authenticated by MITIGATOR Challenge-Response method within HTTPS and redirection to a special verification server

TLS Protection

MITIGATOR allows the protection of TLS applications without traffic decryption by using various methods of the analysis of TLS parameters and JA3 fingerprints. In combination with other countermeasures and a web server log analyzer, it is possible to achieve maximum protection efficiency

MITIGATOR Challenge-Response

A specialized user authentication protocol employing the Challenge Response method, convenient for embedding in a protected application. Supports operation over TCP and UDP protocols. Read more

Fragmented traffic procession

MITIGATOR can collect fragmented traffic for further procession with rules allowing to describe which fragments should be collected and which to be dropped without procession. This creates efficient protection against fragmented traffic attacks

Gaming servers protection

MITIGATOR protects game servers from DDoS attacks via TCP and UDP protocols. The product implements protection mechanisms for Counter Strike: GO and other games from Valve, as well as Minecraft, Rust, ARK, Source Engine Query, etc. New protection mechanisms are added constantly

System event notifications

MITIGATOR can send notifications about system events via email, syslog and Telegram. The user chooses on which events to be notified

Protection of specific protocols

MITIGATOR contains countermeasures that allow you to describe the characteristic behavior of the protected protocol traffic and set sender authentication rules

Programmable filter

Custom traffic processing programs can be created and used in MITIGATOR.

Protection against carpet attacks

MITIGATOR can block traffic senders if they try to access an unusually large number of services. The counting of requests is carried out independently for TCP and UDP

sFlow

MITIGATOR can send sFlow on incoming and outgoing traffic with different sampling values

Dashboards

MITIGATOR web interface allows for the creation of dashboards with a custom number of widgets, containing graphs and statistics, so the users can quickly switch between several sets of widgets and solve various tasks

MITIGATOR DDOS PROTECTION

Syslog Drops

MITIGATOR can send syslog messages about each dropped network packet of specified countermeasures and policies for subsequent analysis in SIEM systems

PCAP

MITIGATOR enables manual and automatic collection of traffic dumps and is able to send them to the user via e-mail and Telegram or post them on a file storage

Bulk Changes

MITIGATOR provides the ability to apply the same action to several selected protection policies at once

Incidents

MITIGATOR keeps detailed logs of changes in traffic characteristics, recognized as attacks. Periodic delivery of incident reports in protection policies is implemented, as well as subscription to notifications about system events

Easy to manage

One screen is used for the setup of countermeasures and monitoring of their effectiveness, without the need to switch between pages of the web interface

Documentation

The MITIGATOR web interface has detailed user documentation in English. The documentation is available both as a summary description and contextually for each element