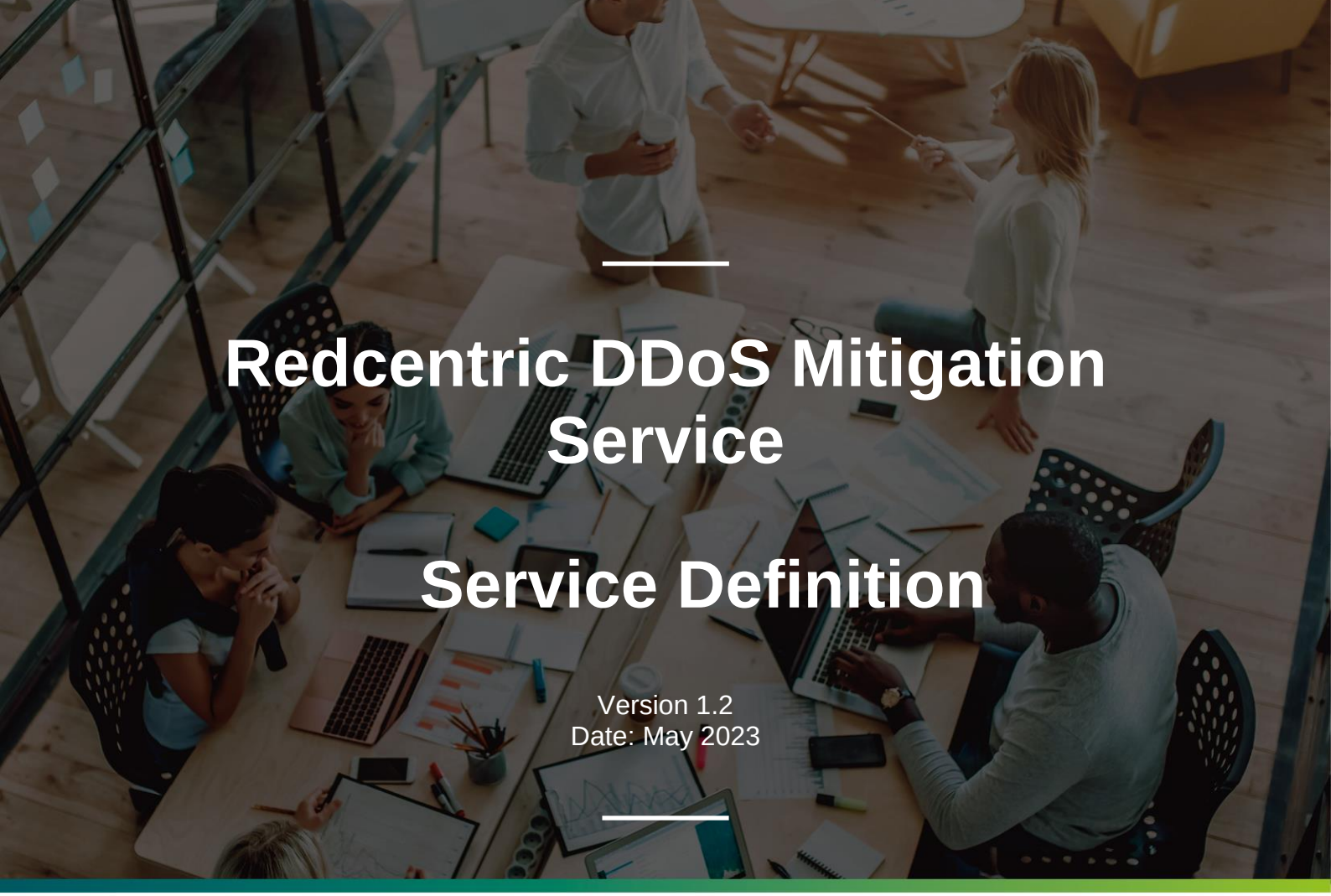


Redcentric DDoS Mitigation Service

Service Definition

Version 1.2
Date: May 2023

redcentric

AGILE • AVAILABLE • ASSURED

1 Service Overview

1.1) Introduction and overview

Distributed denial of service, DDoS is a type of cyberattack that attempts to make online services unavailable by flooding them and / or any or all upstream network assets with malicious traffic where an attacker overwhelms its target with unwanted internet traffic so that normal, legitimate traffic cannot reach its intended destination or be processed successfully. Remember that it's relatively rare a web site is targeted directly.

During a DDoS attack, attackers may use large numbers of exploited machines and connected devices across the Internet including Internet of Things (IoT) devices, smartphones, personal computers, and network servers to send a flood of traffic to targets.

A DDoS attack on a company's website, web application, network, or data centre infrastructure can cause downtime and prevent legitimate users from buying products, using a service, getting information, or any other access.

How does a DDoS attack work?

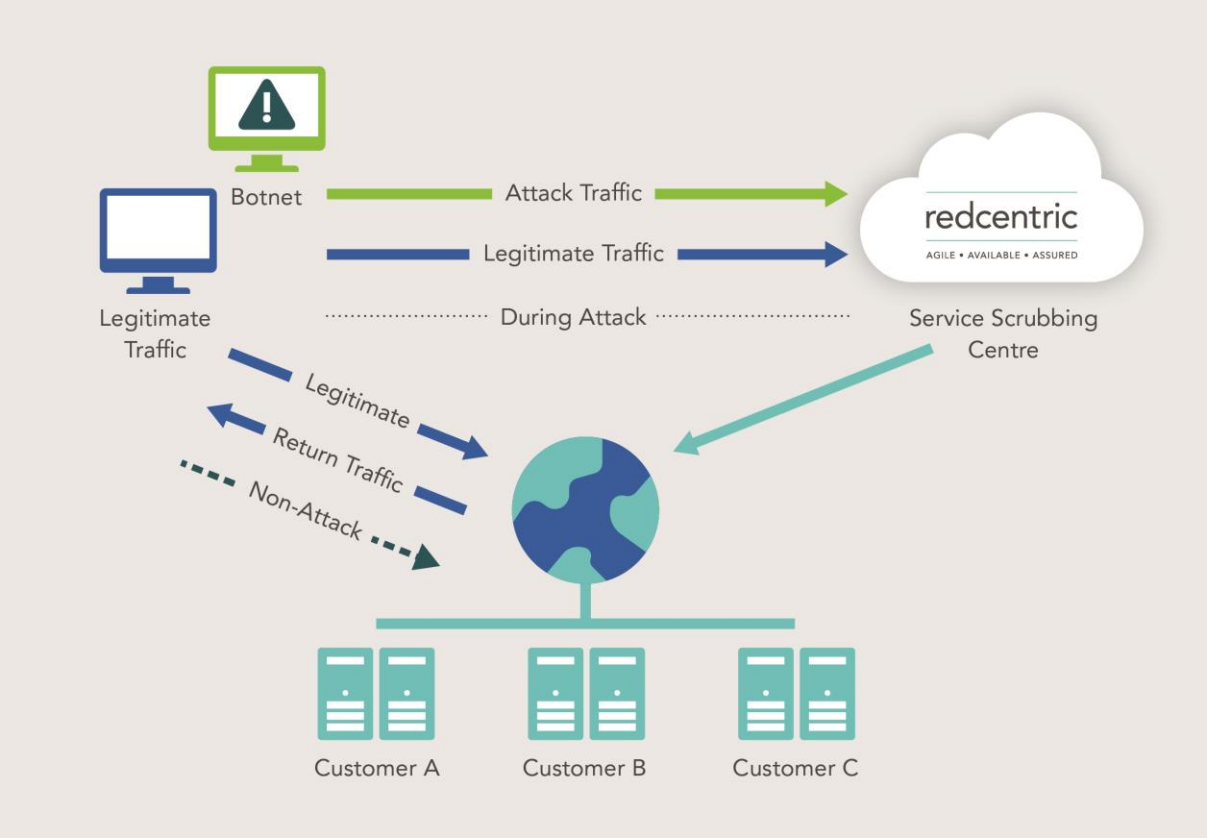
DDoS attacks exploit networks of Internet-connected devices to cut off users from a server or network resource, such as a website or access to any online service application they may frequently access.

2 Service Description

2.1 Service Overview

The Redcentric DDoS Mitigation service provides multiple service levels which caters for any size of customer, ranging from a small business with a minimal online presence to a large enterprise with a significant online presence. These are broken down into 3 service packages.

Redcentric DDoS



DDoS Essentials and DDoS Essentials Plus are very similar in that they are both a reactive service and require the customer to contact Redcentric when they suspect that they are being targeted by a DDoS event, the couple of key differences are that DDoS Essentials Plus offers the ability to activate the DDoS service pre-emptively when a plausible threat has been received, in addition providing basic reporting capabilities. These service packages are only suitable for dealing with a volumetric type of event.

Once notified of a DDoS event, Redcentric will offload the traffic into the on-net scrubbing centre or if very large >1Gb to an upstream scrubbing service, mitigating the volumetric traffic and passing the cleaned traffic back into the network to be routed on to the customer. Outbound traffic will not return via scrubbing centre but be sent out of the customers' default traffic path.

The DDos Pro service package is a fully managed Enterprise grade DDoS mitigation solution which includes a rapid automated response to DDoS attacks by providing immediate detection and mitigation capability. This design and approach reduce risk to the Customer by ensuring full Layer 3-7 mitigation protection.

Redcentric's DDoS mitigation service provides protection for both volumetric and sophisticated attacks along with being able to monitor all inbound and outbound traffic for the detection of DDoS attacks and redirect any traffic for scrubbing to specialised equipment, hosted both in the Redcentric Internet infrastructure and large upstream providers.

A major advantage of this service is that no network changes or configuration is required for a customer to become protected, all the traffic is analysed and scrubbed at the service provider level when required. There is no need for complex tunnels or any peering to be established between the Redcentric network and the customer.

During normal 'peace' time, traffic will flow in and out of the Redcentric network via normal service. If attack traffic detected or Redcentric see a High-Level Alert. Redcentric will offload the traffic into the on-net scrubbing centre, mitigating the volumetric traffic and passing the cleaned traffic back into the network to be routed on to the customer. Outbound traffic will not return via scrubbing but be sent out of the customers' default path. When a DDoS attack is detected our scrubbing service will reroute the IP address under attack directing just traffic destined for that IP to be cleaned, all remaining traffic will pass to the customer. Multiple IP's can be mitigated concurrently.

This service monitors the flow of data from the Redcentric Internet edge routers using Netflow. The routers are configured to send the flow data to the service flow collectors via dedicated links. Because traffic is monitored at the ISP (internet service providers) level, Redcentric gain visibility of the traffic into the customer network allowing us to determine when any attacks begin.

The dedicated links are used to pass the cleaned traffic back to the network. This design allows for zero touch configuration upon customer mitigation.
DDos Essentials and DDos Essentials Plus have a predefined mitigation policy that is non customisable. If a customer takes the DDoS Pro Service package a mitigation policy is designed to meet customer requirements, which is a is a bespoke set of enabled countermeasures assigned to a managed object which is applied as the default set of rules in the event of a DDoS attack. This allows for whitelist/blacklists to be applied immediately, unused ports and protocols to be blocked and much more. In the appendix is a list of the available countermeasures, any one of them can be applied to a mitigation template.

2.2 Key features and benefits

The Redcentric DDoS Mitigation service will provide:

- Bespoke attack thresholds reviewed by Redcentric. *
- Tailored mitigation templates ensuring optimised performance when attacks are mitigated. *
- Mitigations are continually updated to ensure DDoS traffic is scrubbed and 'clean' legitimate traffic is passed successfully back into the customer network.
- Monthly reports and annual service reviews.*

*Service package dependant

2.3 Levels of Service

	Standard	DDoS Essentials	DDoS Essentials Plus	DDoS Pro
Response Time	Black Hole	60 minutes	15 Mins	Automatic
Reactive Service	n/a	Yes	Yes	Always On
Shared Policy	n/a	Yes	Yes	No
Dedicated Policy	n/a	No	No	Yes
Periodic Reporting	No	Yes, Quarterly	Yes, Monthly	Yes, Monthly
Incident Reporting & Analysis	Cost Option	Cost Option	Cost Option	Included (1 Annually)
Edge ACL's	No	No	No	Optional
External Mitigation	Redcentric Black Hole	Yes >5Gb	Yes >5Gb	Yes >5Gb

2.4 Service Implementation

Standard

- Customers IPv4 public address space is added to the Black Hole policy.

The service is delivered by a Redcentric engineer who will be appointed as part the project plan.

DDoS Essentials

- Customer IPv4 public address space is added to the DDos Essentials policy.
- Customer contacts verified and tested.

The service is delivered by a Redcentric engineer who will appointed as part the project plan.

DDoS Essentials Plus

- Customer IPv4 public address space is added to the DDoS Essentials DDoS policy.
- Customer contacts verified and tested.
- Reporting configured, enabled, and tested / confirmed.

The service is delivered by a Redcentric engineer who will appointed as part the project plan and will work alongside the customers technical representative to define the required bespoke policy.

DDoS Pro

A pre-requisite to deployment is a technical information gathering exercise. Information required to deploy the Service includes but is not limited to the following aspects:

- Service Mitigation templates
- Contact details for report recipient(s).
- Customer Technical Representative contact information.

A Redcentric Project Manager will engage with the Customer and establish a project plan. The Project Manager coordinates procurement/ordering, configuration, deployment, testing and hand-over tasks.

The service is delivered by a Redcentric engineer who will appointed as part the project plan and will work alongside the customers technical representative to define the required bespoke policy.

If the Configurations / templates are to be deployed by a Redcentric engineer, installation. Configuration, and basic testing will be undertaken between 9:00am and 17:00pm. Deployment work outside of these hours can be accommodated with explicit up-front agreement in writing by both parties prior to finalising a Service Agreement.

2.5 Customer Responsibilities

Standard

No customer responsibilities.

DDoS Essentials

- Contact details for report recipient(s).
- If the customer suspects that a DDoS event is underway in their environment, the customer informs Redcentric of this occurrence via the normal Redcentric support contact channels.

Please note, Redcentric may engage the service earlier if the level of traffic causes, or risks causing network disruption in any way.

DDoS Essentials Plus

- Contact details for report recipient(s).
- If the customer suspects that a DDoS event is underway in their environment / has received a plausible threat of an impending DDoS event occurring, the customer informs Redcentric of this via the normal Redcentric support contact channels.

Please Note, Redcentric may engage the service earlier if the level of traffic causes, or risks causing network disruption in any way.

DDoS Pro

- The customer will work with Redcentric to define the mitigation template for the required service.
- Contact details for report recipient(s).
- Customer Technical Representative contact information.
- The customer will provide Redcentric with up-to-date list of staff authorised to submit change requests.

Please Note, DDoS Pro is an automated service; therefore, no input is needed from the customer with regards to the ‘normal operation’ of this service.

2.6 Redcentric Responsibilities

Redcentric are responsible for the following aspects of the service:-

- Configuration of the DDoS Mitigation Service and the associated systems.
- Management / upgrade / patching, reporting and Change Management.
- Alerting platforms.
- Notify Customer of high severity incidents.
- Provide reporting dependent on service level.
- Provide IP addresses seen in significant attacks such that the customer can report to the Police.
- Service Availability.
- Routing traffic during incidents to the mitigation platform.

Redcentric will work with all customers of the DDoS Pro service to produce, agree, and implement a service design based on information supplied by the Customer.

2.7 Monitoring

Redcentric will monitor the DDoS mitigation platform to ensure Redcentric can meet the defined service levels.

2.8 Reporting

Standard

- No service reporting included.
- Incident Analysis (available as a PS exercise) / Advanced Incident Reporting.

DDoS Essentials

- Scheduled Quarterly Reporting of DDoS events.
- Incident Analysis (available as a PS exercise) / Advanced Incident Reporting.

DDos Essentials Plus

- Standard Incident reporting.
- Incident Analysis (available as a PS exercise).

DDoS Pro

- Monthly Scheduled Reporting of DDoS events.
- Incident Analysis (1 included annually, additional can be provided as a PS exercise) / Advanced Incident Reporting.

2.9 Incident Management

When a high severity event is triggered or identified and validated by a member of the Redcentric support team, an interaction is raised. Tickets are managed by Redcentric's operations centre 24x365.

If the issue relates to an element not supplied by Redcentric, Redcentric will notify the Customer contact in accordance with the Customer Welcome Pack. Redcentric does not deal with customers 3rd-party suppliers directly.

2.10 Maintenance Notice and Scheduled Downtime

To provide a robust service, Redcentric occasionally performs upgrade and maintenance tasks on systems and platforms. Details of maintenance windows and how they are communicated are detailed in Redcentric's Customer Welcome Pack and Master Service Agreement documents which should be read in-conjunction with this document.

2.11 Change Notice

Redcentric occasionally updates and improves services and adds new features as it strives to provide Customers relevant and valuable services. The Redcentric Master Service Agreement details the implications of Service Change and how it will be communicated.

2.12 Customer requested Changes (DDoS Pro Only)

Redcentric support staff manage the configuration of the DDoS Mitigation service, evaluating and implementing formal change requests submitted by the Customer.

The evaluation and subsequent implementation or rejection of change requests will be performed Monday to Friday between 8 am and 6 pm, with a target completion time of 48 hours for routine changes where a scheduled date/time is not agreed. Emergency changes are prioritised accordingly, and performance targets are detailed in Redcentric's Standard Service Level Targets and Priorities document.

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If Redcentric's security engineer cannot validate the change requester against the authorised list, then Redcentric will place the change request on hold and attempt to contact one of the alternative authorised contacts.

Redcentric must wait for the request to be ratified by a known authorised contact before proceeding with any service change.

It is extremely easy to weaken service integrity and/or security by submitting a seemingly innocuous change request. Redcentric staff review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for service weakness resulting from rule-base changes.

If Redcentric support staff believe that a change in mitigation policy request compromises the security of the Customer's network, Redcentric may ask the Customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered. In extreme cases, staff reserve the right to reject the change outright; for example, if the weakness could affect other Redcentric Customers.

3 Implementation and Acceptance

3.2 Acceptance Criteria

Acceptance Criteria applicable to the DDoS Mitigation Service are listed below:-

DDoS Essentials

- Confirm Redcentric Support contact details have been supplied.
- Contact details for report recipient(s) have been received from the customer and verified.

DDoS Essentials Plus

- Confirm Redcentric Support contact details have been supplied.
- Contact details for report recipient(s) have been received from the customer and verified.

DDoS Pro

- Confirm Redcentric Support contact details have been supplied.
- Contact details for report recipient(s) have been received from the customer and verified.
- DDoS Mitigation policy defined and implemented.
- Test the functionality and notification mechanisms of the service.

4.1 Service Availability

Service Level: Availability Measurement Period: Month	
DDoS Mitigation Service	Not less than 99.5%

4.2 Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded:

- Unavailability due to tasks required to implement and test change requests.
- Unavailability due to scheduled maintenance windows.

5 Service Levels and Service Credits

5.1 Service Level

The service level applicable to the Redcentric DDoS Mitigation service in respect of availability shall be 99.5% in any given month.

5.2 Service Credits

The Service Credits applicable to the DDoS Mitigation service shall be calculated as follows.
In the following table:
"≥" means "greater than or equal to".
"<" means "less than".

Applicable Service	Service Availability	Service Credit
DDoS Mitigation	≥99.5%	none
	≥99.0% but <99.5%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS

"MS" means the charges payable in respect of the DDoS Mitigation Service for the same month.

5) Data Processing

5.1 Data Processing Scope

- Redcentric's DDos Mitigation Service delivers a degree of IP network perimeter protection.
- Redcentric's DDoS Mitigation Service may involve the storage of summarised traffic and user activity.

5.2 Data Storage and Encryption

- By the very nature of the Service, it is necessary for Redcentric to capture, inspect, analyse, and store summaries the Customer's traffic flow data. It is possible that unencrypted packet headers may be stored during an active mitigation.
- Redcentric would not have access to the content of the Customer's traffic/data in normal circumstances. Under certain circumstances, when managing a support ticket, Redcentric may further capture, inspect, analyse and/or store samples of the Customer's traffic in order to investigate and diagnose specific problems

5.3 Data Processing Decisions

- Redcentric does not make any data processing decisions in relation to the Redcentric DDoS Mitigation Service. Any processing of data over Customer systems when using the Redcentric DDoS Mitigation Service is instigated, configured, and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Redcentric DDoS Mitigation Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4 Sub-processors

- Redcentric's DDoS Mitigation Service may make use of services provided by its validated partners. These services assist with the identification and mitigation of security vulnerabilities, weaknesses, exploits, virus, worms etc.
- No other parties are involved in delivering the Redcentric DDoS Mitigation Service, and no other sub-processors are appointed by Redcentric.

5.5 Customer Access to Data

The Customer controls its own platforms which use Redcentric DDoS Mitigation Service, and the Customer therefore has full access to its own data.

5.6 Security Arrangements and Options

The Redcentric DDoS Mitigation Service may be hosted at both Redcentric and third-party locations. All Redcentric appointed locations meet physical security standard ISO27002 section 11.1.

6.0 Appendix 1

IPV4 COUNTERMEASURES

Policy	Description
Invalid Packets	Drops invalid Packets
IPv4 Address Filters	Uses address filters to block
IPv4 Black/Whitelists	Uses black and whitelists to allow or deny
IP Location Filter Lists	Block or Deny based on GeoIP
Zombie Detection	The Zombie Detection countermeasure uses configured threshold values to identify and block hosts (“zombies”) that send excessive amounts of IPv4 traffic to protected hosts or networks. This packet-based countermeasure can protect against common attacks including flood, TCP SYN, and protocol attacks. It should be noted that this mitigation may cause disruption to aggregated traffic such as a VPN concentrator or firewalls
Per Connection Flood Protection	The Per Connection Flood Protection countermeasure monitors IPv4 traffic on a per-connection basis (5tuple) rather than on a per-source basis. When the IPv4 traffic of any connection exceeds the maximum configured rates for bps or pps, then the countermeasure can block all of the traffic of that connection or limit the rate of the traffic of that connection.
TCP SYN Authentication	The TCP SYN Authentication countermeasure intercepts and authenticates all inbound IPv4 and IPv6 TCP connections to the protected hosts. It can protect against TCP SYN flood attacks and any TCP flag attack, such as ACK floods or illegal TCP flag combinations. In these attacks, the TCP protocol is misused to consume a target’s resources. In this countermeasure, the TMS appliance acts as a proxy for the protected hosts to verify that the source host completes a three-way SYN/ACK handshake. If the source host is authenticated, then that host is approved and allowed to connect to the protected hosts. The host remains approved until it does not send a TCP packet within the configured timeout period. If the source host is not authenticated, it is assumed to be malicious, and the connection is not allowed. A host that fails TCP SYN authentication is not blacklisted; any subsequent TCP connection attempt can be used to authenticate that host. Note: If you enable DNS Authentication in Active TCP mode, then TCP SYN Authentication is disabled for port 53.
DNS Scoping	Inspects each request and compares reg-ex to a query and is applied to DNS counter measures
DNS Authentication	The DNS Authentication countermeasure authenticates DNS requests before they reach the DNS server and drops the requests that cannot be authenticated within a specified time. This countermeasure can protect your network against spoof attacks, which occur when an attacker spoofs multiple source addresses in an attempt to overload a DNS server with queries. This countermeasure filters traffic at the packet level.
TCP Connection Limiting	The TCP Connection Limiting countermeasure limits the number of concurrent TCP connections that can originate from a single host. This countermeasure prevents attacks that overwhelm the victim's connection resources with an excessive number of TCP connections. The TCP Connection Limiting countermeasure mitigates IPv4 attack traffic. For example, some botnets open hundreds of active or inactive TCP connections. A sufficiently substantial number of connections can consume all of the resources of a server and prevent the server from accepting legitimate traffic.
TCP Connection Reset	The TCP Connection Reset countermeasure tracks established TCP connections and drops the traffic when a connection remains idle for too long. This countermeasure can prevent idle TCP connections from filling server connection tables. This countermeasure also allows you to blacklist hosts that send extremely slow requests. Although TCP Connection Reset is primarily event-driven, it includes per-packet monitoring of TCP packets so that TCP packet fragments are detected both to reset idle timers and to detect highly fragmented slow application requests.
Payload Regex	Regex checked against the payload data
Source /24 Baselines	No Longer Used

Protocol Baselines	The Baseline Enforcements countermeasure helps protect your network from uncharacteristic surges in traffic volume. For this countermeasure, Peakflow SP collects historical traffic data from the configured managed object. If traffic rates exceed a calculated baseline threshold, then the TMS appliance dynamically blacklists the traffic.
DNS Malformed	Malformed DNS Packets
DNS Rate Limiting	The DNS Rate Limiting countermeasure limits the number of DNS queries that a host can send per second. This countermeasure prevents attacks from legitimate hosts who misuse DNS requests to flood DNS servers. After a host is authenticated, this countermeasure monitors the DNS queries from the source IP address. Any traffic that exceeds the configured rate limit is dropped and the source is blacklisted.
DNS NXDomain Rate Limiting	The DNS NXDomain Rate Limiting countermeasure monitors response packets for hosts that send requests that might cause non-existent domain (NXDomain) responses to be generated. This countermeasure protects against DNS cache poisoning and dictionary attacks. Any host that generates more consecutive failed DNS requests than the configured limit is blacklisted. This countermeasure requires that the TMS appliance be configured in the following ways: ● The appliance must be deployed inline to receive requests and responses. This allows it to detect and correlate the domain-specific relationship. ● The appliance's mitigation capability option must be enabled on both the input and output interfaces.
DNS Regex	Regex checked against the payload data
HTTP Malformed	Malformed HTTP Packets
HTTP Scoping	Inspects each request and compares reg-ex to a query and is applied to HTTP countermeasures
HTTP Rate Limiting	The HTTP Rate Limiting countermeasure limits the rates at which a host can send HTTP requests. This countermeasure prevents a host from overwhelming the resources of a Web server, either by sending too many requests or by requesting too many unique objects. After a host is authenticated, this countermeasure monitors the HTTP requests from the source IP address. Any traffic that exceeds either of the configured rate limits is dropped and the source host is blacklisted. The default HTTP rate limits are usually acceptable for typical users. Because a Web server can be heavily loaded by a small number of HTTP requests, do not increase the limits by substantial amounts without careful consideration. If you must make an exception for a content mirror server, you can add it to a pass rule in the Black / Whitelist filter.
AIF and HTTP/URL Regex	Regex checked against the URL (Uniform Resource Locator) Structure
SSL Negotiation	Monitors SSL Handshakes
SIP Malformed	Drops Malformed SIP Packets
SIP Request Limiting	Limit on number of concurrent or per second SIP Requests
Shaping	Traffic Shaping
IP Location Policing	When you enable IP Location policing rate suggestions on a managed object, Peakflow SP creates per-country traffic baselines that you can use to mitigate the managed object's traffic. This countermeasure allows you to mitigate traffic by doing the following: ● allowing all traffic to enter your network from either specified or unspecified (Other) countries All "allowed" traffic is not necessarily passed. Some allowed traffic could ultimately be dropped as the result of other enabled countermeasures. ● blocking all traffic from entering your network from either specified or unspecified (Other) countries ● limiting (rate shaping) the rate of traffic that enters your network from either specified or unspecified (Other) countries

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED