

DDoS Protection

KNOWLEDGE BASE - NOVEMBER 2026

IN THIS GUIDE

01 Service overview
02 FlexDetect
03 Delivery and traffic diversion
04 Protected prefixes, Zones, and templates
05 Service tiers
06 Burst usage and billing
07 Detection, notification, and management
08 Clean-traffic delivery
09 Responsibilities
10 Service levels and support

> This document is an informative description of the standard Inter.link DDoS Protection service. The applicable service order, Service Level Agreement (SLA), and Master Services Agreement (MSA) prevail in the event of any conflict.

01

Service overview

Inter.link DDoS Protection detects malicious customer-bound traffic, diverts affected traffic to the mitigation platform, applies the selected mitigation policy, and returns clean traffic to the customer. IPv4 and IPv6 prefixes are supported, and detection uses sampled flow telemetry. No learning period is required before automatic detection and diversion can operate.

The service protects inbound traffic. It does not mitigate customer-originated outbound attacks, terminate TLS, provide HTTPS application-layer mitigation, or process customer TLS keys. It is a network-layer protection service rather than a web application firewall or TLS proxy.

Native attachment through IP Transit or IP Access is available at every Inter.link point of presence (PoP). Clean-traffic return through FlexTunnel is subject to availability on selected tunnel-termination routers and must be confirmed in the portal or with Sales. Service availability at a PoP does not mean that the PoP itself is a scrubbing location.

The service order records the delivery model, tier, associated services, term, and charges. Unless otherwise agreed, billing starts when Inter.link provisioning is complete.

02

FlexDetect

FlexDetect is a detection-only edition of DDoS Protection. It gives visibility of DDoS attacks against the customer's prefixes without mitigating them.

When a FlexDetect service is provisioned, a Zone is created automatically and assigned the default monitor template, the only template FlexDetect uses. This template applies the detection settings of the `Default` template with every control in Monitor mode. Attacks are detected, reported by email, and recorded in the

Mitigation portal, but attack traffic is not dropped and no sources are blocked. Other templates, including mitigating and custom templates, are not available with FlexDetect.

The default monitor template applies to FlexDetect Zones only. A new Zone in the full DDoS Protection service starts on the `Default` template, which mitigates.

03

Delivery and traffic diversion

DDoS Protection may be integrated with an Inter.link IP service or return clean traffic over FlexTunnel. The available activation methods depend on the underlying service.

DELIVERY MODEL	AUTOMATIC DIVERSION	BGP-COMMUNITY DIVERSION	ALWAYS-ON DIVERSION
IP Transit	Yes	Yes	Available subject to Inter.link approval
IP Access	Yes	No	Available subject to Inter.link approval
FlexTunnel	Yes	Yes	Available subject to Inter.link approval

Automatic diversion is triggered by attack detection and may be disabled by Inter.link staff. Where a customer BGP session is available, the designated DDoS community forces diversion and overrides the automatic-diversion setting. When the community is removed, the prefix returns to its normal path. The exception is a prefix with automatic diversion enabled while an attack is still meeting the automatic-diversion criteria: it remains diverted until the attack is no longer detected.

Always-on protection uses an engineer-configured static diversion route and is available at Inter.link's discretion. Routing diversion and mitigation policy are independent: a prefix can remain on the mitigation path while its Zone or an individual attack method is in Monitor mode.

When FlexTunnel is used for clean return, the customer establishes BGP with Inter.link over the GRE tunnel. The FlexTunnel specification defines the tunnel's routing, MTU, and availability characteristics.

04

Protected prefixes, Zones, and templates

A protected prefix must be authorized by an applicable customer IRR route object. There is no product-defined minimum or maximum prefix length.

Prefixes are assigned to Zones. Each Zone contains one or more prefixes and applies a mitigation template. An exact prefix can belong to only one Zone, while overlapping prefixes may be assigned to different Zones; the more-specific prefix takes precedence.

Zones, prefix assignments, and mitigation settings can be managed in the Mitigation portal or through the API. Removing a prefix from protection causes its traffic to bypass mitigation.

Templates define how TCP, UDP, ICMP, fragmented, DNS, invalid, and other traffic is handled. The DDoS Protection Templates specification describes the standard templates. The exact available controls are confirmed through Sales or a customer-portal support ticket. A customer can bypass mitigation by placing a Zone in Monitor mode or changing an individual attack method from Auto to Monitor.

05

Service tiers

ATTRIBUTE	PLUS	PREMIUM	ENTERPRISE
Attack-bandwidth tier	1 Tbps	2 Tbps	5 Tbps
Scrubbing-capacity tier	100 Gbps	250 Gbps	500 Gbps
Included protected-prefix billing units	4	10	20
Native IPv6	Included	Included	Included
Best-practice filter	Included	Included	Included
Attack alerting and Mitigation portal	Included	Included	Included
Custom templates	Paid option	5 included	10 included
Allowlist / blocklist entries	1 / 1	5 / 5	10 / 10
FlowSpec	Paid add-on	Paid add-on	Paid add-on

Attack bandwidth is the peak malicious ingress traffic measured before filtering and aggregated per protected service. Scrubbing capacity is the total dirty-side traffic measured across the scrubbing devices for that service. These values are not hard traffic caps: sustained or repeated use above the ordered tier may, at Inter.link's discretion, require a service limitation or package upgrade.

Protected prefixes, custom templates, and allowlist and blocklist entries beyond the tier's included number, including custom templates on the Plus tier, can be used on a burst basis. Burst usage is charged at the applicable per-day rate, as described in Burst usage and billing.

06

Burst usage and billing

IPv4 prefixes are measured in `/24` units and IPv6 prefixes in `/48` units. Each prefix included in the billing calculation contributes independently, including overlapping prefixes. Contributions from both address families are summed and the result is rounded up once to the next whole billing unit. For example, two IPv4 `/25` prefixes together constitute one unit, while one IPv4 `/23` constitutes two.

Prefixes assigned to a Zone using a Monitor template are excluded from the allowance and billing-unit calculation. Changing only an individual attack method to Monitor does not exclude the Zone. The chargeable count for each UTC day is based on the highest enabled unit count sustained for the applicable qualification period; momentary activation does not by itself create a daily overage. Units above the tier allowance are used on a burst basis and charged at the applicable per-day rate. The base service charge continues when every Zone is in Monitor mode.

Custom templates and allowlist and blocklist entries are measured the same way. The chargeable count for each UTC day is based on the highest number configured and sustained for the applicable qualification period, and anything above the tier's included number is charged at the applicable per-day rate.

07

Detection, notification, and management

An email is sent when an attack is detected, and multiple notification recipients can be configured. Attack details and history are available in the Mitigation portal.

All customer mitigation controls available in the Mitigation portal are also available through the API. These include Zone and prefix administration and template management. API access uses a customer-generated API key; formats, scopes, versioning, and limits are defined in the current API documentation.

08

Clean-traffic delivery

Clean traffic is returned over the ordered Inter.link IP service or FlexTunnel. Source and destination addresses are preserved; Inter.link does not perform NAT or proxying. Only inbound traffic is scrubbed, and routing may therefore be asymmetric.

RETURN SERVICE	CLEAN-RETURN CAPACITY
IP Transit	Customer physical-port capacity
IP Access	Customer physical-port capacity
FlexTunnel	Available end-to-end capacity between Inter.link and the customer

09

Responsibilities

ACTIVITY	INTER.LINK	CUSTOMER
Detection and diversion	Operates detection and routing diversion within the ordered scope	Maintains reachable contacts and provides the information necessary for the selected activation model
Mitigation policy	Operates the scrubbing platform and applies authorized settings	Selects suitable templates and assesses false-positive and application impact
Prefix authorization	Validates the configured protected-prefix scope	Maintains accurate IRR route objects and authorization data
Portal and API	Provides the Mitigation portal, API, and support investigation	Secures portal accounts and API keys and controls authorized users
Clean return	Returns clean traffic over the ordered service	Configures and operates the receiving IP service or FlexTunnel

10

Service levels and support

Availability and performance commitments, incident priorities, response and restoration targets, maintenance rules, exclusions, remedies, and service credits are defined exclusively in the applicable SLA. Nothing in this informative specification changes those terms.

Need a hand?

Our network engineers are happy to help — reach out through the Inter.link Portal or visit inter.link.