

DDoS Protection Best Practices

KNOWLEDGE BASE - NOVEMBER 2026

IN THIS GUIDE

01 How DDoS Protection works
02 Getting traffic to the platform
03 Groups, Zones, and templates
04 Before you begin
05 Set up the Mitigation portal
06 From Monitor to Mitigate
07 Choosing a template
08 Everyday operations
09 During an attack
10 Automating with the API
11 Adding FlowSpec
12 Service tiers and billing units
13 Who does what
14 Getting support
15 Glossary

> This document describes best practices for setting up and operating the Inter.link DDoS Protection service. It is practical guidance, not a service definition. The DDoS Protection, DDoS Protection Templates, FlowSpec, BGP Communities, and Mitigation Portal API specifications define the service. The applicable service order, Service Level Agreement (SLA), and Master Services Agreement (MSA) prevail in the event of any conflict.

This guide is for the network and operations engineers who will configure and run DDoS Protection for their organisation or their own customers. It assumes familiarity with BGP, IP prefixes, and basic traffic analysis.

IF YOU WANT TO...	READ
Understand the service before go-live	How DDoS Protection works; Getting traffic to the platform; Groups, Zones, and templates
Set up the Mitigation portal for the first time	Before you begin; Set up the Mitigation portal; From Monitor to Mitigate
Pick or change a mitigation template	Choosing a template
Handle routine portal tasks	Everyday operations
Respond to an attack in progress	During an attack
Automate or filter at the edge	Automating with the API; Adding FlowSpec

01

How DDoS Protection works

Inter.link DDoS Protection detects attacks against your prefixes, moves the affected traffic onto the mitigation path, scrubs it, and returns the clean traffic to you.

STAGE	WHAT HAPPENS
Detect	Sampled flow telemetry from the Inter.link edge is analysed continuously. No learning period is needed, so detection works from day one.
Divert	Traffic for the affected prefix is moved onto the mitigation path: automatically, by your BGP community, or permanently (always-on).
Mitigate	The scrubbing platform applies the template assigned to the prefix's Zone and drops traffic that the template classifies as attack traffic.
Return	Clean traffic is delivered over your Inter.link IP Transit, IP Access, or FlexTunnel service.

Only inbound traffic is scrubbed. Source and destination addresses are preserved, with no NAT or proxying, so return paths may be asymmetric.

What is protected

IN SCOPE	OUT OF SCOPE
Inbound traffic to your IPv4 and IPv6 prefixes	Outbound attacks originating from your network
Volumetric, protocol, and state-exhaustion attacks (TCP, UDP, ICMP, fragments, DNS, invalid packets)	TLS termination or HTTPS application-layer mitigation; you never share TLS keys
Selected plain-text application behaviour, such as abnormal HTTP methods	Web application firewall functions

Diversion and mitigation are independent

Two separate settings decide what happens to a packet. Diversion decides whether traffic is on the mitigation path at all. The template and its mode decide what the platform does with traffic once it is there.

A prefix can be diverted while its Zone is in Monitor mode. You then get full visibility and alerts, but nothing is dropped. The reverse also holds: a Zone in Mitigate mode does nothing for traffic that is still on the normal path.

02

Getting traffic to the platform

There are three ways to put traffic on the mitigation path:

- **Automatic** is the default. Traffic is diverted when an attack is detected and returns to its normal path when the attack is no longer detected. It has the least latency impact and needs no action from you.
- **BGP community** diversion forces a prefix onto the mitigation path when you tag it with `65535:700`. It overrides the automatic setting and suits integration with your own tooling.
- **Always-on** diversion uses a static route configured by an Inter.link engineer, so traffic is always scrubbed. It is available subject to Inter.link approval.

Which methods you can use depends on the underlying service:

DELIVERY MODEL	AUTOMATIC	BGP COMMUNITY	ALWAYS-ON
IP Transit	Yes	Yes	On approval
IP Access	Yes	No	On approval
FlexTunnel	Yes	Yes	On approval

Using the diversion community

Announce the prefix to Inter.link with `65535:700` attached. The prefix stays diverted for as long as the community is present. For example, with illustrative router syntax:

```
route-map TO-INTERLINK permit 10
 match ip address prefix-list UNDER-ATTACK
 set community 65535:700 additive
```

> **Tip:** When you remove the community, the prefix returns to its normal path. The exception is when automatic diversion is enabled and an ongoing attack meets the automatic-diversion criteria. The prefix then stays diverted until the attack is no longer detected.

Clean-traffic return

RETURN SERVICE	CLEAN-RETURN CAPACITY	NOTES
IP Transit	Your physical-port capacity	Available at every Inter.link PoP
IP Access	Your physical-port capacity	Available at every Inter.link PoP
FlexTunnel	End-to-end capacity between Inter.link and you	BGP runs over the GRE tunnel; selected termination routers only

Service availability at a PoP does not mean that the PoP is itself a scrubbing location.

03

Groups, Zones, and templates

Everything you configure in the Mitigation portal is built on three objects. Getting this structure right at the start saves work later.

Groups are the unit of ownership. A Group holds Zones and optional sub-groups, and it is where users, alert recipients, and reports are defined. Users of a Group can see and manage everything beneath it, so Groups are the natural way to separate business units or, for partners, individual customers.

Zones tie one or more prefixes to a single template, and every prefix in the Zone is treated the same way. An exact prefix can belong to only one Zone, but prefixes may overlap across Zones, and the more specific prefix wins. This lets you watch a whole aggregate in one Zone while giving specific hosts their own policy.

A typical structure looks like this:

```
Group: Example Networks          (users, alerting, reporting)
 ├── Zone: Aggregates              Monitor template, catch-all
 │    198.51.100.0/22
 │    2001:db8::/32
 ├── Zone: Web platform            Mitigate-WebHosting-Balanced-v001
 │    198.51.100.0/24
 └── Zone: DNS servers             Mitigate-DNSHosting-Balanced-v001
      198.51.101.53/32
```

Traffic to `198.51.100.0/24` and `198.51.101.53/32` is handled by their own Zones because they are more specific than the `/22` aggregate.

Templates are pre-configured mitigation policies. Each covers protocol policy, packet validation, SYN flood detection, session abuse, UDP floods and reflection, DNS validation, ICMP floods, fragment handling, and HTTP detection. Each of those controls runs in one of three modes:

MODE	BEHAVIOUR
Auto	Mitigates when its detector triggers
Force on	Mitigates continuously, whether or not an attack is detected
Monitor	Detects and reports, but does not drop traffic

Every Mitigate template has a Monitor version with identical detection settings, for example `Mitigate-CDN-Balanced-v001` and `Monitor-CDN-Balanced-v001`.

> **Tip:** Every Group and Zone is something to maintain. Start with an aggregate catch-all Zone, and add dedicated Zones only for services that need different treatment, such as frequent targets or UDP-heavy services.

04

Before you begin

Most setup delays come from missing route objects or unclear prefix lists. Check the following before your first login:

- ☐ **Service order confirmed.** You know your tier, delivery model, and which diversion methods apply.
- ☐ **IRR route objects in place.** Every prefix you want to protect is covered by an applicable route object. Prefixes without one cannot be protected.

- [ ] **Prefix inventory.** You have a list of aggregates and of the services inside them that need special treatment, such as DNS, anycast, CDN, QUIC/HTTP/3, GRE, VoIP, or gaming.
- [ ] **Contacts.** You have named the portal users and the email addresses that should receive attack alerts and reports.
- [ ] **BGP ready**, if you will use the community. You can attach `65535:700` to announcements towards Inter.link.
- [ ] **Clean return working.** For FlexTunnel, the GRE tunnel and its BGP session are up.

Then plan your structure. Sketch your Groups and Zones using the example above as a model, and for each Zone note its prefixes, its traffic profile, and the template family that matches it.

ZONE	PREFIXES	TRAFFIC PROFILE	STARTING TEMPLATE

05

Set up the Mitigation portal

> **Important:** A new Zone starts on the `Default` template, which is not monitor-only: it mitigates. As soon as a prefix is added to a Zone, the Zone's template applies to it. Always assign a Monitor template to the Zone before adding prefixes that attract traffic, so that nothing is dropped until you have reviewed the results.

FlexDetect, the detection-only edition of DDoS Protection, works differently. Its Zone is created automatically on the default monitor template, and other templates are not available. The template and mitigation steps in this guide apply to the full DDoS Protection service.

Build the structure

1. Sign in to the Mitigation portal with your Inter.link customer portal account. Accounts are synced between the customer portal and the Mitigation portal.
2. Create any sub-groups you planned. Skip this if a single Group is enough.
3. In the relevant Group, create your first Zone and give it a descriptive name, such as *Aggregates* or *Web platform*.
4. Assign a Monitor template, for example the Monitor version of the template you chose, such as `Monitor-WebHosting-Balanced-v001`. The Zone now detects and reports only.
5. Repeat for each planned Zone.

Add prefixes

1. Open each Zone and add its prefixes or host addresses.
2. Add the aggregate catch-all prefixes last, so that the more specific Zones are in place when traffic starts to be classified.
3. Check that each prefix appears in the expected Zone.

Set up alerts, reports, and users

1. At Group level, add the email recipients for attack alerts. You can add several.
2. Schedule daily, weekly, or monthly reports and choose their recipients. Reports can also be generated on demand and downloaded from the portal.
3. Add the colleagues who need portal access to the Group, with the roles they need.

An alert is sent when an attack exceeds the template's reporting threshold. It identifies the target Group, Zone, and IP; the attack types; the Zone's filter mode; the start time and duration; and the attack, dropped, current, and peak volumes in packets and bits. The same detail is available in the portal's attack history. Reporting thresholds keep normal background noise out of your inbox, so a quiet first day is normal.

06

From Monitor to Mitigate

A Monitor template shows exactly what its Mitigate version would drop against your real traffic, without dropping anything. It is the safest way to find false positives before they affect users. The default monitor template applies the detection settings of the `Default` template with every control in Monitor mode. The Monitor version of a specific template shows how that template would behave. The FlexDetect section of the DDoS Protection specification describes the default monitor template.

Prefixes in a Zone that uses a Monitor template do not count towards your protected-prefix billing units. Setting only an individual attack method to Monitor does not exclude the Zone.

Review a Zone in Monitor mode

1. Let the Zone run in Monitor mode long enough to see representative traffic, including your normal peaks.
2. Open the Zone's traffic view and check how much traffic is classified as attack traffic. Outside a real attack, there should be next to none.
3. Open the Zone's filter list and check which sources would have been blocked. Look for your own monitoring systems, partners, and large customers.
4. If legitimate traffic is flagged, try the Loose template of the same family, or contact Inter.link about a custom template.

Switch to Mitigate

1. Starting from the Group, select the Zones to switch. You can change several Zones at once.
2. Assign the Mitigate version of the same template, for example `Mitigate-WebHosting-Balanced-v001`. Detected attack traffic is now dropped, and offending sources may be blocked for the template's block time.
3. Watch the Zone for the next few hours and check its filter list again.

> **Tip:** You can keep a Zone in Mitigate mode and set a single attack method to Monitor. This is useful when one control misbehaves for your traffic while you investigate.

07

Choosing a template

Pick a family that matches the traffic, then a sensitivity level that matches your appetite for risk. Template names follow this pattern:

```
Mitigate-WebHosting-Balanced-v001
 |         |           |         └── version
 |         |           └── sensitivity: Loose, Balanced, or Strict
 |         └── network family
 └── Mitigate (drops) or Monitor (reports only)
```

NETWORK OR SERVICE	START WITH
General or mixed traffic	`Default` or `Base-Mitigate-0202`
Anycast services	`Mitigate-Anycast-Balanced-v001`
Content delivery	`Mitigate-CDN-Balanced-v001`
Multi-tenant cloud or virtual servers	`Mitigate-CloudHosting-Balanced-v001`
Content providers, including GRE traffic	`Mitigate-ContentProvider-Balanced-v001`
Authoritative or recursive DNS	`Mitigate-DNSHosting-Balanced-v001`
Websites and HTTP services	`Mitigate-WebHosting-Balanced-v001`
Services using QUIC or HTTP/3	The Loose template of the matching family

LEVEL	USE WHEN	TRADE-OFF
Loose	Availability comes first, or traffic is bursty or unusual	Slower, less aggressive containment
Balanced	Recommended starting point for most networks	Middle ground

LEVEL	USE WHEN	TRADE-OFF
Strict	Attacks are not contained quickly enough	Higher risk to borderline legitimate traffic

> **Important:** Balanced and Strict templates in every family, all Cloud Hosting templates, and `Base-Mitigate-0300` drop UDP to and from port 443, which includes QUIC. The `_Drop-UDP` templates drop all UDP. Check this before applying them to services that use QUIC, HTTP/3, DNS, VoIP, VPN, or gaming.

All standard templates except the Under-Attack templates are available for self-service. Contact Inter.link only when a template does not work as intended or when you need a new custom template, which is chargeable. The DDoS Protection Templates specification describes every template in detail.

08

Everyday operations

Find traffic, attackers, and victims

Use the portal search to look up a victim IP or prefix, a known attacker, blocked sources, top talkers, or allow and block list entries.

> **Important:** Keep the time range as narrow as possible and include a specific source or destination address. Wide searches and long graph ranges are slow and can make your browser stop responding.

Release a blocked source

In Mitigate mode, some controls block offending source addresses for a set time, from 60 minutes in the Base templates to several hours in Strict templates.

1. Search for the source IP, or open the filter list of the Zone concerned.
2. Confirm the entry, the control that blocked it, and when the block expires.
3. Release the entry. Traffic from the source is accepted again unless it triggers a detector again.
4. If the same legitimate source is blocked repeatedly, consider a source allow list entry or a looser template.

Change a Zone's template or mode

The quickest route is from the Group, where you can assign a new template to several Zones at once. To change the mode of a single attack method instead, edit the Zone's configuration and set that method to Auto, Force on, or Monitor.

Allow and block lists

Lists accept IPs and prefixes. A source allow list entry skips DDoS analysis for the specified protocols, so use it sparingly. Entries by autonomous system or country code, and forcing the SYN flood control on, are coordinated with Inter.link and used only during an active attack.

Routine checks

HOW OFTEN	CHECK
Weekly	Read the scheduled report: attack breakdown, top attacks, and protocol distribution
Monthly	Review the filter list for repeat legitimate blocks, and remove stale list entries, portal users, and API keys
On change	When you add a service or prefix, decide its Zone before announcing it, and keep IRR route objects current

09

During an attack

Work down these steps until the impact stops:

1. **Confirm the target.** Check the alert or the portal's list of Zones under attack. Note the target IP, Zone, attack types, and current volume.
2. **Check diversion.** Mitigation only applies to diverted traffic. If the traffic is not on the mitigation path, force it with `65535:700` where your service supports the community.
3. **Check the mode.** If the Zone or the relevant attack method is in Monitor mode, switch it to Mitigate.
4. **Tighten the template.** If the attack is not contained, move the Zone to the Strict template of its family.
5. **Escalate.** If the impact continues, open a support ticket. For TCP-based attacks, Inter.link can apply an Under-Attack template in coordination with you.
6. **Filter at the edge (optional).** If you have FlowSpec, a narrowly scoped rule can drop or rate-limit a clear signature before it reaches the scrubbing stage.

Under-Attack templates are emergency profiles with maximum sensitivity. They drop all UDP and all IP protocols other than TCP and ICMP, and block offending sources for 960 minutes or more. They are applied only in coordination with Inter.link through a customer-portal support ticket, and they are unsuitable for DNS, VoIP, VPN, gaming, or QUIC services.

When the attack is over:

- [ ] Return the Zone to its regular template.
- [ ] Remove the `65535:700` community if you added it.
- [ ] Withdraw any FlowSpec rules you advertised.
- [ ] Remove temporary allow or block list entries.

- [ ] Release legitimate sources that were blocked.
- [ ] Record the timeline and keep the attack details for your incident report.

10

Automating with the API

Every control in the Mitigation portal is also available through its REST API, with the same permissions.

Create an API key from your user profile in the Mitigation portal. The key carries your roles and permissions. The token is shown only once, so store it in your secrets manager straight away. Keys do not expire; delete a key to revoke it. Send the key on every request:

```
Authorization: token <API key>
```

Typical uses include pulling Zone traffic statistics into your own monitoring, listing Zones with historical attacks above a threshold, retrieving top attacking sources, maintaining block and allow lists, and changing a Zone's filter mode as part of an automated response.

TOPIC	BEHAVIOUR
Paging	`start_row` (from 1), `number_of_rows`, `sort_name`, and `sort_order`; results are wrapped in `data`
Long-running requests	Return `202 Accepted` with a job; poll `GET /delayed_job_statuses/{id}` until `finished` is true
Errors	`401` means authentication or permission failed; `422` lists invalid fields
Changes	Take effect on live mitigation immediately; Zone configuration is revisioned
Upgrades	The API follows portal releases; re-validate integrations after an upgrade

The full endpoint reference is the rWeb API developer guide. The Mitigation Portal API specification describes access, scope, and fair use. Never include API keys in tickets or logs.

11

Adding FlowSpec

FlowSpec is a separately ordered add-on that lets you filter traffic at the Inter.link edge yourself, using BGP. It has no detection or managed mitigation: you write the rules, advertise them, and withdraw them. It complements DDoS Protection by stopping a known signature at the edge.

Packets are handled in this order, and a packet dropped at an earlier stage never reaches the later ones:

1. Any matching FlowSpec rule, at the receiving edge
2. DDoS diversion, if applicable

3. Normal routing

ITEM	DETAIL
Eligible services	IP Transit and FlexTunnel, using the existing BGP sessions (AFI 1 and 2, SAFI 133), with at least 10 Gbps aggregate commitment per service type
Every rule needs	A destination prefix that you are authorised for; source-only rules are silently filtered
Actions	Rate limit in bytes per second, drop (rate 0), or accept; one action per rule
Enforcement	Applied on every AS5405 edge router; rate limits are policed per router, not network-wide
Visibility	No portal or API view and no traffic counters; verify the effect in your own monitoring

> **Important:** Unsupported rules are filtered silently, without a BGP error. Rules never expire on their own, so withdraw them when the attack is over. The FlowSpec specification lists the supported match components.

12

Service tiers and billing units

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

Protected prefixes are counted as follows:

- IPv4 is counted in `/24` units and IPv6 in `/48` units. Each prefix counts on its own, including overlapping prefixes.
- Both address families are summed and rounded up once. Two IPv4 `/25` prefixes make one unit; one IPv4 `/23` makes two.

- Prefixes in Zones using a Monitor template are excluded.
- Usage above your tier is allowed on a burst basis and charged per day, based on the highest count sustained for the qualification period.

Attack bandwidth and scrubbing capacity are not hard caps. Sustained use above the ordered tier may require a service limitation or package upgrade. The DDoS Protection specification gives the full billing rules.

13

Who does what

AREA	INTER.LINK	YOU
Detection and diversion	Operates detection and diversion within the ordered scope	Keeps contacts reachable and provides what the chosen diversion method needs
Mitigation policy	Operates the scrubbing platform and applies authorised settings	Selects templates and assesses false-positive and application impact
Templates	Maintains the standard library, investigates templates that do not work, and coordinates Under-Attack templates	Chooses a template per Zone and changes it as traffic or threats change
Prefix authorisation	Validates the protected-prefix scope	Maintains accurate IRR route objects
Portal and API	Provides the portal, API, and support investigation	Secures accounts and API keys and controls who has access
Clean return	Returns clean traffic over the ordered service	Configures and operates the receiving IP service or FlexTunnel
FlowSpec	Distributes valid rules on a best-effort basis	Writes, verifies, and withdraws rules

14

Getting support

Open a ticket in the customer portal. For emergencies, use the contact route and priorities defined in your SLA.

Contact Inter.link when:

- An attack is not contained after following the steps in During an attack
- You need an Under-Attack template, or allow or block list entries by AS or country, during an attack
- A template does not work as intended, or you need a new custom template
- You want always-on diversion

Include the following in every ticket:

- Affected Group, Zone, and target IP or prefix
- Start time and, if it is over, end time, preferably in UTC
- What you observe and what you expected
- The current template and mode, and any recent changes
- For FlowSpec: the NLRI, timestamps, and traffic evidence
- For API issues: the endpoint, method, response code, and redacted request and response

Remove API keys, passwords, and other secrets from anything you send to support.

15

Glossary

TERM	MEANING
Always-on	Permanent diversion of a prefix through the mitigation platform using a static route
Attack method	One detection control within a template, such as SYN flood or UDP flood; each has its own mode
Auto, Force on, Monitor	The modes of an attack method: mitigate on detection, mitigate continuously, or report only
Clean return	Delivery of scrubbed traffic back to your network
Diversion	Moving a prefix's inbound traffic onto the mitigation path
Filter list	Sources currently blocked by a control in Mitigate mode
FlowSpec	BGP-signalled filtering rules applied at the Inter.link edge
Group	Container for Zones, users, alerting, and reporting
IRR route object	A registry entry authorising your ASN to originate a prefix; required for protection
Monitor template	A template with every control in Monitor mode; excluded from prefix billing
Template	A pre-configured mitigation policy applied to all prefixes in a Zone
Zone	A set of prefixes sharing one template; more specific prefixes win across Zones

Need a hand?

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