

DDoS Protection Templates

KNOWLEDGE BASE - OCTOBER 2026

IN THIS GUIDE

01 Overview
02 What a template controls
03 Sensitivity levels
04 Mitigate and Monitor versions
05 Base and Default templates
06 Network-specific templates
07 Under-Attack templates
08 Templates for use in coordination with Inter.link
09 Attack reporting
10 Selecting a template
11 Custom templates
12 Responsibilities

> This document is an informative description of the standard mitigation templates offered with the 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

Overview

A mitigation template is a pre-configured DDoS Protection policy. Each Zone in the DDoS Protection service applies one template to all of its prefixes, so a customer can protect a network by choosing the template that matches its traffic profile instead of building mitigation rules from scratch.

Zones, prefix assignments, and template selection are managed in the Mitigation portal or through the API. The DDoS Protection specification describes Zones, traffic diversion, service tiers, and billing.

02

What a template controls

Every template configures the same set of controls. Templates differ in which controls are active, how sensitive their detectors are, and how long offending sources are blocked.

CONTROL	FUNCTION
Protocol policy	Whether UDP, TCP, ICMP, and other IP protocols are accepted
Packet validation	Drops packets with invalid lengths, flags, fragment bits, checksums, null addresses or ports, and malformed IPv6 extension headers
TCP SYN flood detection	Detects random and targeted SYN floods and validates connection setup

CONTROL	FUNCTION
TCP session-abuse detection	Detects and optionally blocks sources that hold idle sessions open, churn RST closes, send duplicate ACKs, use very small windows, or send data after a session has closed
UDP flood and reflection detection	Detects UDP floods, identical-payload floods, and amplification protocols, validates NTP, and can block specific UDP ports
DNS validation	Validates DNS queries and responses and detects duplicate requests
ICMP flood detection	Detects ICMP and ping floods
Fragment handling	Limits the share of fragmented TCP, UDP, and ICMP traffic
HTTP detection	Detects HTTP fragmentation, abnormal or excessive methods, recursive GETs, and misused or faulty applications

All standard templates drop CHARGEN and QOTD reflection traffic, validate NTP traffic, and validate DNS traffic.

Each control runs in one of three modes. In Auto, the control mitigates when its detector triggers. In Force on, the control mitigates continuously whether or not an attack is detected. In Monitor, the control detects and reports but does not mitigate.

03

Sensitivity levels

Network-specific templates are offered in three levels. Under-Attack templates are separate emergency profiles.

LEVEL	INTENDED USE	TRADE-OFF
Loose	Availability first; tolerates bursts and unusual but legitimate traffic	Slower or less aggressive containment
Balanced	Recommended starting point for most networks	Middle ground between availability and containment
Strict	Faster blocking and longer block times	Higher risk of affecting borderline legitimate traffic
Under-Attack	Emergency use during an active attack	Maximum sensitivity, restricted protocols, and the highest false-positive risk

04

Mitigate and Monitor versions

Each network-specific template and each Base template has a Monitor version with identical detection settings. The only difference is that every control is set to Monitor, so the template detects and reports attacks but does not scrub traffic. A Monitor version can be used to evaluate how a template would behave against real traffic before active mitigation is enabled.

MITIGATE TEMPLATE	MONITOR TEMPLATE
`Mitigate–<Network>-<Level>–v001`	`Monitor–<Network>-<Level>–v001`
`Base-Mitigate-0202`	`Base-Monitor-0202`
`Base-Mitigate-0300`	`Base-Monitor-0300`

Prefixes in a Zone using a Monitor template are excluded from the protected-prefix billing calculation, as described in the DDoS Protection specification. Changing only an individual attack method from Auto to Monitor does not exclude the Zone.

05

Base and Default templates

TEMPLATE	BEHAVIOUR
`Default`	Conservative general-purpose profile. All detectors run at standard sensitivity. Session-abuse detection runs without blocking sources. Fragmented traffic and SSDP are accepted and no UDP ports are blocked.
`Base-Mitigate-0202`	General-purpose profile with raised sensitivity for SYN floods, UDP floods, and HTTP abuse. Session-abuse blocking is enabled with a 60-minute block time. Fragmented traffic and SSDP are accepted and no UDP ports are blocked.
`Base-Mitigate-0300`	High-sensitivity profile for earlier containment. SYN, UDP, ICMP, and HTTP detectors run at high sensitivity with long HTTP block times. Drops UDP traffic to and from port 80, UDP from source port 11211 (memcached), and UDP to and from port 443 (including QUIC). SSDP and DNS queries with no question are rejected. Session-abuse blocking matches `Base-Mitigate-0202` with a 60-minute block time.

06

Network-specific templates

The six network families share stricter packet hygiene than the Base templates: fragmented TCP is limited to 1% of traffic, fragmented ICMP is dropped, and SSDP is rejected. Except in the DNS Hosting family, TCP ECN flags are validated.

Balanced and Strict templates in every family, and all Cloud Hosting templates, drop UDP from source port 11211 (memcached) and UDP to and from port 443. Services that rely on QUIC or HTTP/3 should use a Loose template or a custom template.

Session-abuse block times referred to below are the time a source detected by the TCP session-abuse detector remains blocked.

Anycast

The levels differ only in TCP session-abuse handling and UDP port blocking. Volumetric and HTTP detectors run at standard sensitivity in all three.

TEMPLATE	BEHAVIOUR
`Mitigate-Anycast-Loose-v001`	Session-abuse blocking enabled at moderate sensitivity with a 60-minute block time. No UDP ports blocked.
`Mitigate-Anycast-Balanced-v001`	Aggressive session-abuse detection with a 240-minute block time.
`Mitigate-Anycast-Strict-v001`	Aggressive session-abuse detection at higher sensitivity with a 480-minute block time.

CDN

The CDN family has the most permissive session handling: sources are detected but not blocked for session abuse. Volumetric and HTTP detectors run at standard sensitivity in all three levels. The levels differ in the share of fragmented UDP accepted and in UDP port blocking.

TEMPLATE	BEHAVIOUR
`Mitigate-CDN-Loose-v001`	Up to 15% fragmented UDP accepted. No UDP ports blocked.
`Mitigate-CDN-Balanced-v001`	Up to 10% fragmented UDP accepted.
`Mitigate-CDN-Strict-v001`	Up to 5% fragmented UDP accepted.

Cloud Hosting

All three levels apply aggressive session-abuse blocking with a 240-minute block time, raised HTTP detection sensitivity, and UDP port blocking. The levels differ only in SYN flood detection.

TEMPLATE	BEHAVIOUR
`Mitigate-CloudHosting-Loose-v001`	Relaxed SYN flood detection for bursty multi-tenant connection patterns.
`Mitigate-CloudHosting-Balanced-v001`	Standard SYN flood detection.
`Mitigate-CloudHosting-Strict-v001`	Raised SYN flood detection sensitivity.

Content Provider

All three levels apply raised UDP flood and HTTP detection sensitivity. GRE (IP protocol 47) is accepted and the inner headers of tunnelled traffic are not inspected. The levels differ in session-abuse handling, fragmented UDP, and UDP port blocking.

TEMPLATE	BEHAVIOUR
`Mitigate-ContentProvider-Loose-v001`	Session-abuse blocking at moderate sensitivity with a 60-minute block time. Up to 15% fragmented UDP accepted. No UDP ports blocked.
`Mitigate-ContentProvider-Balanced-v001`	Aggressive session-abuse detection with a 240-minute block time. Up to 10% fragmented UDP accepted.
`Mitigate-ContentProvider-Strict-v001`	Aggressive session-abuse detection at higher sensitivity with a 480-minute block time. Up to 5% fragmented UDP accepted.

DNS Hosting

All three levels accept only TCP, UDP, and ICMP; other IP protocols are dropped. Session-abuse sources are detected but not blocked, and HTTP detectors run at standard sensitivity. The levels differ in UDP flood sensitivity, fragmented UDP, and UDP port blocking.

TEMPLATE	BEHAVIOUR
`Mitigate-DNSHosting-Loose-v001`	Slightly raised UDP flood sensitivity. Up to 15% fragmented UDP accepted. No UDP ports blocked.
`Mitigate-DNSHosting-Balanced-v001`	Raised UDP flood sensitivity. Up to 10% fragmented UDP accepted.
`Mitigate-DNSHosting-Strict-v001`	High UDP flood sensitivity with earlier activation. Up to 5% fragmented UDP accepted.

Web Hosting

All three levels apply raised HTTP detection sensitivity with standard UDP flood detection. The levels differ in session-abuse handling, SYN flood sensitivity, and UDP port blocking.

TEMPLATE	BEHAVIOUR
`Mitigate-WebHosting-Loose-v001`	Session-abuse blocking at moderate sensitivity with a 60-minute block time. Slightly raised SYN flood sensitivity. No UDP ports blocked.
`Mitigate-WebHosting-Balanced-v001`	Aggressive session-abuse detection with a 240-minute block time. Raised SYN flood sensitivity.
`Mitigate-WebHosting-Strict-v001`	Aggressive session-abuse detection at higher sensitivity with a 480-minute block time. High SYN flood sensitivity.

07

Under-Attack templates

Under-Attack templates are emergency profiles for use while an attack is in progress. They must only be applied in coordination with Inter.link, through a customer-portal support ticket, and are not intended for self-service selection. They share the high-sensitivity detection of `Base-Mitigate-0300` and add the following:

- All UDP traffic and all IP protocols other than TCP and ICMP are dropped. These templates are therefore not suitable for services that depend on UDP, such as DNS, VoIP, VPN, gaming, or QUIC.
- Session-abuse detection is aggressive and at very high sensitivity, with block times of 960 minutes or more.

TEMPLATE	BEHAVIOUR
`UNDER-ATTACK-POLICY_v101`	Baseline emergency profile. SYN flood mitigation is forced on, so connection setup is validated continuously rather than only when an attack is detected. Session-abuse block time is 960 minutes.
`UNDER-ATTACK-POLICY_v101_AT8-max`	As `UNDER-ATTACK-POLICY_v101`, with session-abuse detection at maximum sensitivity, lower bad-session thresholds, and a 1,440-minute block time. Intended for session-exhaustion attacks; carries the highest false-positive risk.
`UNDER-ATTACK-POLICY_v101-no-forceOn`	As `UNDER-ATTACK-POLICY_v101`, but SYN flood mitigation runs in Auto mode and activates only when a SYN flood is detected.
`UNDER-ATTACK-POLICY_v101-no-forceon2`	Identical in settings to `UNDER-ATTACK-POLICY_v101-no-forceOn`.

A Zone should be returned to its regular template once the attack has subsided.

08

Templates for use in coordination with Inter.link

The following templates are very specific profiles. They must only be applied in coordination with Inter.link, through Sales or a customer-portal support ticket, and are not intended for general self-service selection. The Under-Attack templates described above are subject to the same requirement.

TEMPLATE	BEHAVIOUR
`Base-Mitigate-0202_Drop-UDP`	As `Base-Mitigate-0202`, but all UDP traffic is dropped.
`Base-Mitigate-0202_Drop-UDP_SYN-Force-ON`	As `Base-Mitigate-0202_Drop-UDP`, with SYN flood mitigation forced on. Intended only for TCP-only services.
`FlexdetectTemplate`	Settings identical to `Default` with every control in Monitor mode. It detects and reports attacks but does not mitigate them.

09

Attack reporting

Templates also define when a detected attack is reported. `Default` and `FlexdetectTemplate` report most attack types once the attack has lasted 10 minutes. The other standard templates report most attack types as soon as the attack meets the packet-rate threshold. Notification recipients are configured as described in the DDoS Protection specification.

10

Selecting a template

NETWORK OR SERVICE	SUGGESTED STARTING POINT
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-carrying 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
Active TCP-based attack not contained by the current template	An `UNDER-ATTACK-POLICY_v101` variant, in coordination with Inter.link

The Monitor version of the chosen template can be applied first to assess false-positive impact. Moving to a Loose template is appropriate when legitimate traffic is mitigated, and to a Strict template when attacks are not contained quickly enough.

Diversion and template selection are independent. A prefix is mitigated only while its traffic is on the mitigation path, whether through automatic diversion, always-on diversion, or the DDoS redirect BGP community `65535:700` described in the BGP Communities specification.

11

Custom templates

The number of custom templates included depends on the DDoS Protection tier, as listed in the DDoS Protection specification. Custom templates are requested through Sales or a customer-portal support ticket. Custom templates beyond the tier's included number, or on a tier that includes none, can be used on a burst basis and are charged at the applicable per-day rate.

12

Responsibilities

ACTIVITY	INTER.LINK	CUSTOMER
Template library	Maintains and publishes the standard templates	Reviews the available templates and their intended use
Template selection	Applies the template assigned to each Zone and advises on coordination-only and Under-Attack templates	Selects a suitable template for each Zone and changes it as traffic or threats change
Impact assessment	Supports investigation through the Mitigation portal and support	Assesses false-positive and application impact, including through Monitor versions

Need a hand?

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