BaDOS – FAQ v1.0

created by sVen Mueller (s.mueller@f5.com)

What is BaDOS?
It is your friend ;-)
Seriously: Automatically detection Layer 7 (*HTTP*) (D)DoS attacks using behavioral data
Characterize the offending traffic and automatically mitigate on the offending traffic.
Hands off: No need for user intervention: no need to configure thresholds, nor to maintain them.
The ***"engine"*** is self-adjusting and adaptive to changes.
Alert and mitigate even before defended service fails
Improves with experience: The longer it operates the higher the confidence.

Does BaDOS honour X-Forwarded-For header?

Yes, when *Accept X-Forwarded*-For in the http profile is enabled.
Keep in mind L3 mitigation (packet cannot be done based on X-Forwarded –For header).

What mitigation types do BaDOS have and what does that mean?

Conservative Protection:

If "Bad actor's detection" enabled, slows down and rate limit requests from anomalous IP address based on its anomaly detection confidence and the server´s health.
If "Request signatures detection" enabled, blocks requests that match the attack signatures.

Standard Protection:

If "Bad actor's detection" enabled, slows down requests from anomalous IP addresses based on it anomaly detection confidence and the server´s health.
Rate limit requests from anomalous IP address and, if necessary, rate limits all requests based on the server´s health.
Limits the number of concurrent connections from anomalous IP addresses and, if necessary, limits the number of all concurrent connections based on server´s health.
If "Request signatures detection" enabled, blocks requests that match the attack signatures.

Aggressive Protection:

If "Bad actor's detection" enabled, slows down requests from anomalous IP addresses based on it anomaly detection confidence and the server´s health.
Rate limit requests from anomalous IP address and, if necessary, rate limits all requests based on the server´s health.
Limits the number of concurrent connections from anomalous IP addresses and, if necessary, limits the number of all concurrent connections based on server´s health.
If "Request signatures detection" enabled, blocks requests that match the attack signatures.
Increases the impact of the protection techniques.
Proactively performs all protection actions (even before an attack).
Increases the impact of the protection techniques

Mitigation flow

Order	Mitigation	Condition
1	L3 slowdown of bad actors	Operation mode = Blocking Bad actor's behavioural detection enabled Mitigation = conservative/standard/aggressive BAD actors detected (greylist) Under attack (in aggressive mode also before attack)
2	L7 requests rate limit of requests from bad actors	Operation mode = Blocking Bad actor's behavioural detection enabled Mitigation = conservative/standard/aggressive BAD actors detected (greylist) Under attack (in aggressive mode also before attack)
3	Server concurrent connections limit (initiated by bad actors)	Operation mode = Blocking Bad actors behavioural detection enabled Mitigation = standard/aggressive BAD actors detected (greylist) Under attack Server health requires it
4	Server concurrent connections limit (initiated by bad and good actors)	Operation mode = Blocking Bad actor's behavioural detection OR Request signatures detection enabled Mitigation = standard/aggressive Under attack
5	L7 requests drops by signatures enforcer	Operation mode = Blocking Request signatures detection enabled Mitigation = conservative/standard/aggressive Under attack (in aggressive mode also before attack *TBD) Request matched by active signature

Should I enable mitigation from beginning?

Yes, mostly go with the "Standard Protection" mitigation configuration.
You can check the learning status with:

```
# admd -s vs./Common/Hackazon_BaDOS_protected+/Common/Hackazon_BaDOS.info.learning
```

Name of the VS
Name of the DOS profile

The output looks like that:

```
vs./Common/Hackazon_BaDOS_protected+/Common/Hackazon_BaDOS.info.learning:[62.0614, 6, 7061, 100]
```

62.0614	average approximation to the learned baselines
6	number of bins to be measured
7061	the number if learned unique suggestions
100	signatures good dataset is ready

Keep in mind the longer the system runs the better it gets. It is permanently self-adjusting.

How do I know what the status of learned traffic? –When is it ready to mitigate?

The output of **.info.learning** will give you some numbers.

```
vs./Common/Hackazon_BaDOS_protected+/Common/Hackazon_BaDOS.info.learning:[62.0614, 6, 7061, 100]
```

The indication of the readiness is [not 0, any, any, 100]

How do I see if IPs are grey-listed?

```
# ipidr -l /Common/VS+/Common/DOS-Profile
```

How do I delete grey-listed IPs for a DOS profile?

```
# ipidr -c /Common/VS+/Common/DOS-Profile
```

How do I see how BaDOS mitigates

DOS Dashboard, HTTP analytics

```
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.l3actualgreylistpktdrops
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.grey_conns_drops
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.conn_drops
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.l7actualgreylistdrops
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.l7_signature_drops
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.l7actualglobaldrops
```

How do I check the server health?

```
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.health
```

How do I check the incoming request rate?

```
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.l7requests
```

How Do I check TPS rate?

```
# admd -s vs./Common/VS+/Common/DOS-Profile.sig.tps
```

How do I see all signals and other BaDOS traffic properties?

```
# admd -s vs./Common/VS+/Common/DOS-Profile.sig
```

How do I see if the system is under attack?

```
# admd -s vs./Common/VS+/Common/DOS-Profile.info
```

Can I use L3 shunning on grey-listed IPs?

Yes, when using an IPI Policy configured to block the category “Application denial of services” this IPs get shunned.

How Can I use Grafana on my environment?

Go to https://devcentral.f5.com/d/behavioral-ddos-grafana-dashboard-using-big-ip-apis-244
And you will find an instruction on how to install and configure Grafana.

On how many VS can I enable BaDOS?

On ASM it is limited to 2 VS.
On DHD it is limited to 50 VS.
On Advanced-WAF it is unlimited!

Should I use BaDOS in conjunction with any other L7 DOS functionality?

Enabling Bot signatures is in general a good idea. It will block bad and stupid Bots upfront, when blocking on those categories is enabled.

Proactive Bot defence as well, when it is used in always mode. It will not get activated through BaDOS. Only when TPS- or Stress-based DOS reports an attack.

Stress-based and BaDOS running on the same VS usually doesn´t make sense. Both are based on server stress.

TPS-DOS could be used, when for whatever reason something goes wrong and you want to block just based on hard thresholds in order to protect the server.