DEPLOYMENT GUIDE

Advanced DNS Protection

Ruleset Tuning

NIOS 8.4

Table of Contents

Introduction

The Infoblox Advanced DNS Protection (ADP) solution employs threat protection rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service), and other network attacks targeting DNS authoritative and recursive services. Infoblox Advanced DNS Protection helps minimize “false positives” and ensures that your mission-critical DNS services continue to function even whilst under attack.

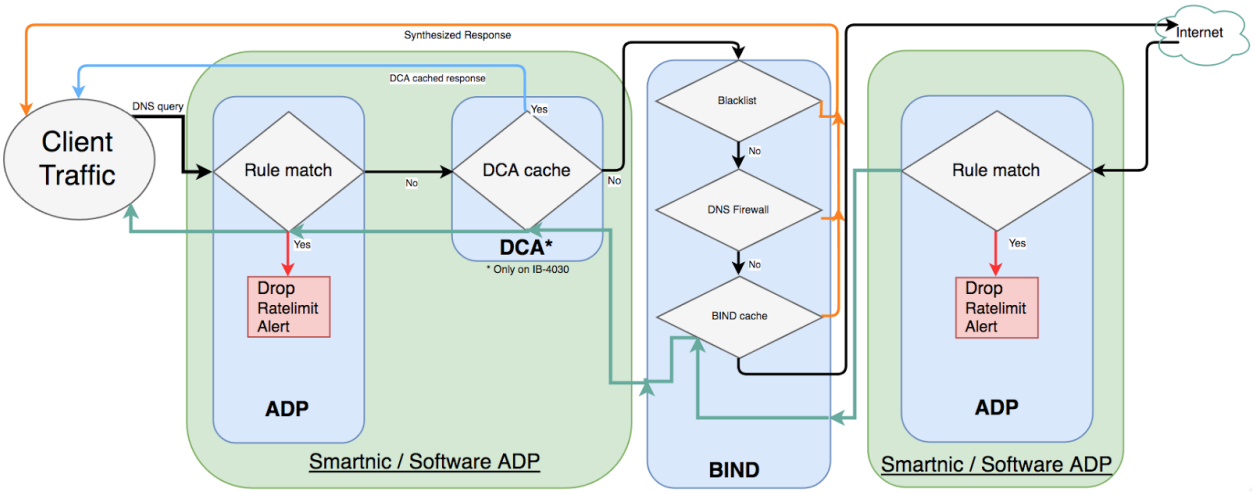
You can deploy the Advanced DNS Protection on hardware-accelerated appliances (physical appliances only) as well as on regular appliances by adding the appropriate license. This allows you to run ADP on both physical and virtual appliances. Depending on the appliances you deploy, you must install applicable permanent or subscription licenses.

Note: the term “ADP” is used to include both appliances with software ADP licenses and physical PT appliances.

Note: We tend to use the term client, a client may be a IP address, or a IP address and a set of ports. This is known as deterministic NAT. The Administrator Guide covers this feature in detail in a section called *Configuring NAT mapping Properties*.

Packet Flow Diagram

The following diagram illustrate how a DNS (and throughout the document) packet is treated when received by the network interface:



The diagram shows the path an incoming packet takes through the systems that are in line.

Beginning with ADP, followed by DCA. It then gets passed on to BIND and then passes the traffic once more through ADP engine on its way to the internet to receive an authoritative response.

The DNS Cache Accelerator (DCA) is available on the IB-4030 platform (physical) and appropriately configured IB-FLEX virtual appliances and is designed for very low latency cache responses. DNS firewall and the BIND cache are more intertwined than is shown in the diagram. Certain configurations require DNS responses to be validated against the DNS firewall rules.

Any response is first processed by the ADP engine, then goes through BIND. It is added to the cache at named level and the response is then parsed by DCA which caches only A, CNAME, PTR, MX and AAAA responses. The final response is once more validated by ADP against a limited set of rules that monitor transactions before being sent to the client.

ADP operation

ADP operation is governed by a ruleset, which is an ordered collection of rules.

A ruleset will evaluate traffic that arrives on the NIC and verify it against all rules until it receives a PASS, or an explicit DROP. If no PASS is received, the traffic will be dropped by the final rules (Ruleset Category “Default Pass/Drop”). Depending on the configuration of the setup, traffic may be rate limited or an alert generated or both.

ADP performs deep packet inspection which examines any protocol that the appliance is configured to service. It will only allow traffic for the protocol services that are enabled, and rules will be enabled or disabled depending on other configuration settings for those services.

For example: If you enable the NTP service on an ADP appliance, then ADP will stop filtering out NTP packets and pass them onto the underlying OS on which NTP is running. It will also enable rules designed to protect the NTP service from attack.

NOTE: Grid communications has to be configured on MGMT interface on the appliance running ADP. Refer to admin guide for details.

Order of operation

ADP rules are applied by their **Order** specified in the UI.

To display the Grid level Threat Rulesets, in the Web UI:

- go to Data Management > Security > Threat Protection Rules,
- click on a ruleset,
- toggle flat view,
- sort by order, Ascending.

If you add custom rules, they have the same value for order and will be evaluated in the order of their “Rule ID”

The following data is analyzed by ADP

- TCP/UDP
    - IP
        - Source IP
        - Destination IP
        - Source Port
        - Destination port
        - Flow bit
        - Application/Service data
            - DNS
                - Header

        - Body
    - BFD
    - BGP
    - DHCP
    - DHCP failover
    - IGMP
    - Kerberos
    - NTP
    - OSPF
    - OpenVPN
    - RADIUS
    - VRRP
- ICMP
- Other traffic is dropped

ADP Actions

Pass

If the packet receives a PASS from a rule it is passed on to NIOS. This is applied on incoming. No log entry gets created.

Alert

If the packet generates an ALERT from a rule, it is passed on to the following rule. This is applied on incoming as well as outgoing traffic. A syslog entry of the configured severity gets created if Events Per Second (EPS) > 0.

Rate limiting

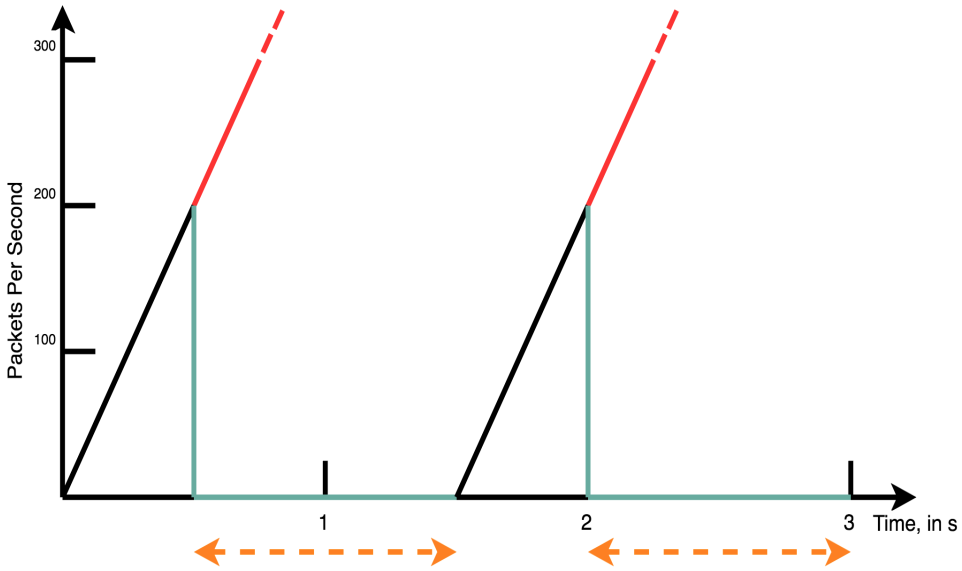
Next to rules based on these parameters there are also rules present which are rate dependent. This means that ADP keeps track of the Packets Per Second count for certain traffic and that a configurable PPS can be let through. Whenever the rate is exceeded a log message is logged if EPS > 0.

ADP has the ability to track the Packets Per Second (PPS) for a rule. When the threshold is exceeded there are a number of actions that can occur for subsequent traffic.

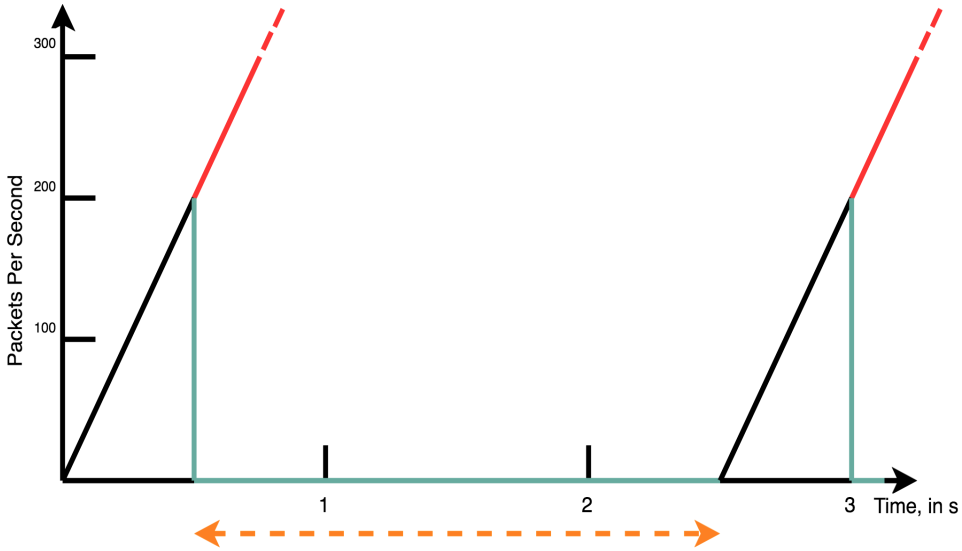
Rate Algorithm

Rate_limiting

When you select this action then no more traffic than the allowed rate is let through before a blocking action occurs. In the diagram below the PPS limit for this rule has been set to 200 and the drop interval (orange arrow) to 1 second. The client is sending over 200 PPS. ADP drops any packets that exceed the configured limit and ignores the client for 1 second. The counter resets one second after the limit has been reached and allows traffic again up to the configured rate.



When you change the drop interval to 2 seconds the pattern becomes:

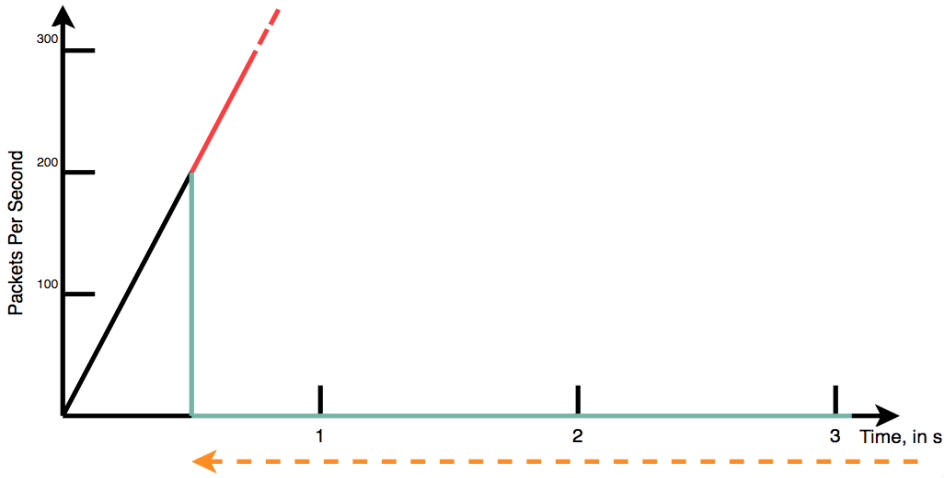


Blocking

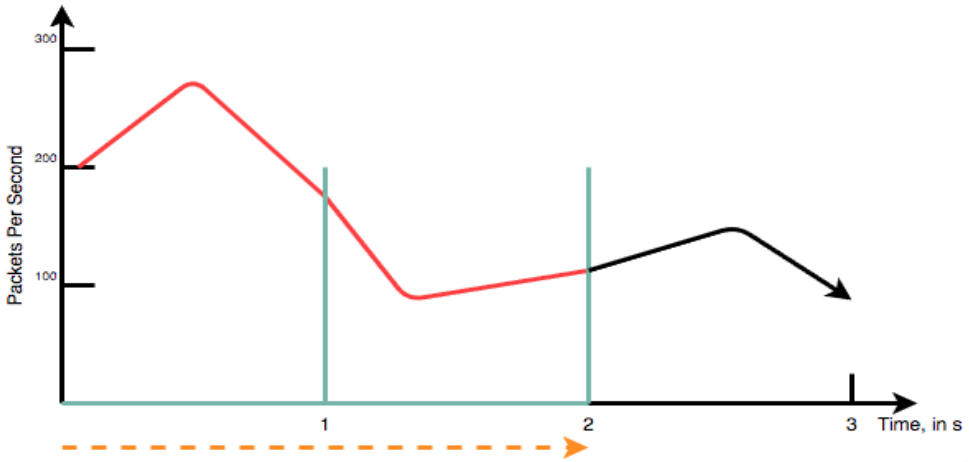
When you set a rule with the rate limiting algorithm set to blocking, client traffic will be blocked for the offending source until

- The client drops below the set limit during the last second of the drop interval
- Other resets of the blocking state happen when
    - a change to any rule is made and published
    - a service restart is done
    - a service on the ADP appliance are disabled or enabled
    - a new ruleset is published

When the Rate Algorithm is set to blocking, blocking will occur for as long as the client exceeds the PPS limit, this is colloquially referred to as the penalty box.



In the following diagram you see what occurs once we approach the end of the blocking period on second 2. The traffic rate during the last second, while still being blocked, is below 200 PPS. This means that as of second 2 traffic will be allowed again. If the traffic goes over 200 PPS again, the block would trigger and remain active until the client drops below the configured value.



Drop

If the packet generates a DROP from a rule, it is immediately dropped. This is applied to incoming traffic. A syslog entry gets created if EPS > 0 that matches the severity set.

Like traditional firewall rules, the default rule is drop, but ADP does distinguish between DNS, and protocol types used by the appliance to assist in debugging.

Monitor mode

You can configure your ADP appliances to operate in a special passthru mode called monitor mode. This mode is enabled from the CLI and is intended to evaluate the effect of a ruleset on traffic. By running in monitor mode traffic is passed through the ruleset without any enforcement. No action is taken on the traffic. Each hit does generate a log event as long as EPS > 0. When a packet encounters a rule and receives a PASS it is not

evaluated by any further rules. Do note that when operating in monitor mode a single packet can trigger multiple rules if these rules are set to ALERT or DROP.

Deploying Rules

Refer to “ADP initial deployment” on how to deploy Rulesets and profiles (see Additional documentation section at bottom)

Reporting Server - Reports to Review

What Data should you be collecting

Reporting prerequisites

In order for the ADP reports to populate with data you require

- A reporting member
- The reporting service running on the reporting member
- The reporting service running on your ADP member
- All categories turned on for enabled services running in your grid
- At least an index percentage of 1% for those categories selected
- The reporting service running successfully for at least 1 week prior to enabling ADP. This will help with initial rate limit tuning values.

Log events per second

There is a global events per second (EPS) setting as well as the ability to override this setting on a per rule basis. Setting this parameter governs “events **per** second **per** client **per** rule”. It means that each client will generate an event each time it hits a rule. If the same client hits a rule multiple times within one second, then the EPS value is taken into account. A client can be either an IP or in case NAT is configured the IP + the port it is mapped to.

As a general rule individual rules value for EPS should be set to either 0 or 1.

- Be aware that if you enable syslog data indexing in the reporting server, and have set high EPS values, you can overload the indexing volume of your reporting server.
- You can also consume all of your appliance’s I/O resources due to large numbers of log events being written to disk. This is colloquially known as “death by syslog”.

How to deal with index overages and reporting license violations

A reporting index overage is when your reporting server indexes more logs in a given day than permitted by the license. If this happens occasionally there will be no impact to your reporting service. If this situation however occurs on 5 days within a 30-day window, then you will not be able to run any more searches. This means that while the data is still being indexed any reports, dashboards and searches will stop working.

If you do require access to your reporting data, then you must contact Infoblox Support. A one-time violation-reset-key can be generated and applied to your environment.

Suggestions on reporting monitoring

After rolling out ADP with reporting it is suggested to monitor both the daily index volumes as well as the storage indexes on a daily basis.

After a week of close monitoring you can move to weekly monitoring, after a month to monthly and after 3 months switch to quarterly.

If you implement any changes that impact the reporting data being indexed, you might want to monitor more frequently.

Alerts

Alerts from reporting server

With reporting you have the ability to craft alerts based on any parameters you like. Refer to the training material on Infoblox Reporting and creating alerts for more information.
Some examples would be:

- DDOS, Amplification, ...
- Alerts when an important internal network triggers and ADP ruleset for a known bad domain.

System alerts

A grid master is able to generate SNMP and email alerts. Since these are real time, they should be configured for the categories that matter to your organization.

- System CPU/Memory/NIC usage
- Cache hit ratio
- NXDOMAIN hits
- Any issues with the status of services (DNS/DHCP/NTP/...)
- Notifications on threat protection dropped traffic and threat protection total traffic

Deployment steps with reporting

What to do prior

If you have an existing Grid, then reporting data even from prior to implementing ADP can be very useful with regards to your later tuning of the rules.

It is also assumed that your architecture has been validated and appropriately designed.

If you are adding ADP to an existing grid, and/or plan to cutover services to ADP appliances then the support from Infoblox Professional Services can be invaluable.

Initial setup and review

During the initial phase of the deployment it is advised to have ADP in monitor mode and ensure that all disabled system rules are evaluated and have Events Per Second set to 1 or if appropriate/default 0.

Note: Some of these rules are more relevant to service provider traffic patterns vs enterprise external authoritative servers.

Monitor mode logs will give a clearer picture of which rules get triggered when you are in production mode. The following reports should be consulted to locate any major issues that are ongoing:

"Threat Protection Top Rules Logged"
"Threat Protection Top Rules Logged by Source"

“Threat Protection Event Count by Rule”
“Threat Protection Event Count by Member Trend”
“DNS Top clients”
“DNS Top NXDOMAIN / NOERROR (no data)”
“DNS Top Clients by Query Type”
“DNS Top SERVFAIL Errors Received”
“DNS Top SERVFAIL Errors Sent”

Based on these reports any flagrant attacks and or attackers can be blacklisted, it may show if there is a need to temporarily whitelist any IP’s and or domains. This mode will allow you to create an initial baseline of the traffic patterns. You might need to whitelist IP’s through which a lot of clients are NATed. If there are enough of these, they can be directed to a different ADP which has a more appropriate profile.

Generally, do avoid whitelisting and be aware that adding entries to the whitelist can cause you to lose visibility into this traffic at later stages. It is most important to understand the reason why you are whitelisting a client. Whitelisting should only be used for short term fixes until you can work out a proper solution. It may be indicative of a need for an architectural review.

During this phase the following search can also help you find those clients you need to take care of:

All IP’s with ADP rule hits report

```
source=ib:ddos:ip_rule_stats index=ib_security                (RULE_SID = * )
| stats count by SOURCE_IP,RULE_SID,RULE_NAME
| lookup dnslookup clientip as SOURCE_IP
| sort -SOURCE_IP
| table SOURCE_IP, clienthost,count, RULE_SID,RULE_NAME
```

Second phase setup

After the major offenders have been filtered out the following rules should be reviewed to match the requirements of the implementation. Once the configuration feels solid it is advised to switch away from monitor-mode. The following categories and rules should be monitored closely in this stage. Any anomalies you detect will allow you to review the hits and their origin. You can then make decisions if you want to address the client triggering rule hits or if you want to introduce custom rules.

DNS Protocol Anomalies

DNS protocol anomalies send malformed DNS packets, including unexpected header and payload values, to the targeted server. This might cause the server to stop responding or crash. These anomalies sometimes take the form of impersonation attacks. These are pattern matching type rules.

Rule 110100600- EARLY DROP UDP query invalid question count

This rule drops UDP DNS packets when the number of entries in the question section is invalid.

Rule 110100900- EARLY DROP UDP query multiple questions or non query operation code

This rule drops UDP DNS packets when there are multiple questions being queried at one time or its operation code is not Query.

Rule 110100700- EARLY DROP UDP query invalid question class

This rule drops UDP DNS packets when the RR (resource record) class being queried is invalid.

Rule 110100800- EARLY DROP UDP query invalid question string

This rule drops UDP DNS packets that contain invalid question string.

Rule 130000700 DNS Protocol Anomalies EARLY DROP TCP non-DNS query

This rule will drop any DNS TCP based packets that are not actual queries

Rule 130000800 DNS Protocol Anomalies EARLY DROP TCP query multiple questions

This rule drops DNS queries over TCP that contain multiple query sections, this is frequently used for DNS tunneling purposes.

Default PASS/DROP

The following table lists the system rules that are used to pass or drop packets on your advanced appliance. All these rules are enabled by default. There are rules in these categories that are the deny any any equivalent in a traditional firewall at the end of the chain. Care needs to be taken to make sure that non RFC compliant requests that are being dropped are not used to as a health check by load balancing systems. These health checks should be fixed/updated. You may need to change the EPS from 0 to 1, or do a packet capture to identify the issue.

Rule 140000600- DROP UDP unexpected

This rule drops any UDP packet on any port. If this rule is triggered, most likely this packet is not intended for services on this member.

Rule 140000100- DROP UDP DNS unexpected

This rule drops any unexpected UDP DNS packets. This means ADP has not found a reason to pass this packet.

Rule 140000200- DROP TCP DNS unexpected

This rule drops any unexpected TCP DNS packets. This means ADP has not found a reason to pass this packet.

Rule 140000500- DROP UDP unexpected

This rule drops any unexpected UDP packets.

Rule 140000600- DROP TCP unexpected

This rule drops any unexpected TCP packets.

Rule 140000700- DROP ICMP unexpected

This rule drops any ICMP packet. If this rule is triggered, most likely this packet is not intended for services on this member.

Rule 140000800- DROP unexpected protocol

This rule drops any unexpected protocol packets; this is the final rule to drop any protocols we do not know and prevents us from passing such traffic onto NIOS.

Potential DDoS Related Domains

This rule category includes system rules the appliance uses to blacklist domains that may have been the targets or subjects in NXDOMAIN or DDoS attacks. These rules block all FQDN lookups on UDP for domains that have been observed as designed to be targets in DDoS attacks. The rules are enabled by default. You can disable them when necessary.

Note that these rules capture currently observed bad domain names that can change on a regular basis. Infoblox recommends that you automatically update to the latest ruleset to capture the most current rules in this category.

Rule 12060***- Potential DDoS related domains

The current list of rules that have hits on the ADP appliance, this is subject to change over time as they are updated in order to block the highest profile and most prolific malicious domains. These domains are often used in sandwich random subdomain attacks whose intent is to bring down recursive DNS servers. In blocking these domains, ADP can also help protect other innocent DNS servers that might be in the recursive path

Potential DDoS related domain: middleseatblues.net

Potential DDoS related domain: nineenterntainmentco.com.au

Potential DDoS related domain: nmfm.com

Potential DDoS related domain: venturas.com.br

Potential DDoS related domain: omplus.ch

Potential DDoS related domain: ontrees.com

Potential DDoS related domain: paylance.ph

Potential DDoS related domain: nucleussec.com

Potential DDoS related domain: regionstest.com

Potential DDoS related domain: stzh.be

ICMP

ICMP attacks use network devices such as routers to send error messages when a requested service is not available, or the remote server cannot be reached. Examples of ICMP attacks include ping floods, ping-of-death attacks, and smurf attacks.

Rule 130903400- RATELIMIT ICMP port unreachable

This rule passes ICMP port unreachable messages if the packet rate is less than the Packets per second value. If any source IP sends packets over this value, the appliance blocks all such traffic from this source IP for the block interval period of time.

Third phase setup

Now that you have a baseline and you have done a first review of your rulesets it is time to dive a little deeper into the way DNS servers are being exploited.

Severity levels

You may wish to update severity levels of rules in order to make the data you provide to your SIEM or NOC more relevant to their operation.

A possible configuration could be:

- Critical: something that **has** to be dealt with in a non automated method, yet something you are capable of remediating as it occurs.
- Major: similar to critical, you may not have a standard remediation, so it needs more investigative work internally to resolve – it may instigate a trouble ticket
- Warning: low grade of Major, later follow up required, it may also instigate a trouble ticket
- Informational: logging to trace origin, ADP is performing the appropriate remedial action.

You also need to review the syslog reporting settings so that your security logs get sent to your security systems. You can find these setting under

1. Grid > Grid Manager > Members
2. Click Grid properties in the right-hand toolbar
3. Click on the monitoring tab
4. Check the box for “log to external syslog servers”
5. Click the Plus Symbox to add an external syslog server
6. Under Logging Category select send selected categories
7. Select:
    - Threat Protection
    - DHCP Process
    - DNS Client
    - DNS Config
    - DNS General
    - DNS Lame Servers
    - DNS Networks
    - DNS Notifies
    - DNS Resolver
    - DNS RPZ
    - DNS Security
    - DNS Unbound
    - DNS Updates
    - DNS Update Security
    - Zone Transfer In
    - Zone Transfer Out

These logs will send provide your SIEM actionable network intelligence.

You can also use outbound notifications if you have the Ecosystem license, see Grid -> Ecosystem and Outbound Endpoint, or Notification

Advanced Rules Tuning

DNS tunneling

Look at packet size and rate, both parameters are tunable.

They can be set to very low values so that any packet over 150 will generate a warning.

The biggest offenders in this category because of packet size are: Sophos, mcafee, spotify, myfreedom, ….

Many domains transport a lot of data via your dns infrastructure.

The default packet size is 200, in the field certain DNS tunnels uses random packet size between 120 - 180.

We have seen tunnel “bundling” taking multiple dns tunnels and bundling them together to get better throughput via the DNS tunnel in applications like Tunnel Guru.

Rules order importance

General UDP and TCP DNS rate limits are the earliest rate limits.

This means that they will proceed any other rate limit rule you configure. As such can effectively never be exceeded. The order of rules is often overlooked. You cannot modify the order of rules.

Different members see different traffic

Leverage profiles with different settings on a per member or per client category basis. Many times, you will encounter client categories like enterprise, subscriber, ...

DNS response rules

There are a number of rules which take into account the response to the query from each client and will block the offending client entirely from making any more DNS queries during the drop interval.

These rules are:
Rule 200000001 NXDOMAIN rate limiting rule
Rule 200000002 NXRRSET rate limiting rule
Rule 200000003 SERVFAIL rate limiting rule

Similar behavior can be seen for Rule 200000004 DNS Tunneling rate limiting rule

This rule will however only drop TXT record response traffic and not all DNS traffic from the client.

Other significant rules

Flood Rules – depending on the QPS (for example, less than 500) you use in 130000100, 130000200, 130000300, 130000400 (which includes its TCP equivalents), you may wish to forgo enabling the 100/300 rules, as these will generate many syslog events. If you set the QPS higher you may use the 100/300 rules as a NOC/SOC alert before drops occur.

It is very important that it is understood that these rules provide the maximum QPS allowed before an action is taken, so setting any other rate limited rule higher will have no effect.

Reflection Attack - Rule 130400100 WARN & DROP DoS DNS possible reflection/amplification attack attempts. This rule should, in general, not be increased over 5 PPS as this allows classic amplification attacks. This is the ANY request it is only used for troubleshooting purposes and should not exceed 1 PPS since only a human should be issuing this request by hand.

Note that Reporting ADP hits does not equal offending packets. It depends if there is a threshold or PPS rate limit that defines "inappropriate behavior" which is just one event caused by some number of packets.

Unicast Reverse Path Forwarding (Unicast RPF)

Unicast Reverse Path Forwarding is designed to help limit malicious traffic in service provider networks. This is a security feature that works by enabling a router to verify the reachability of the source address in the packets being forwarded. This capability can limit the appearance of spoofed addresses on the network. If the source IP address is not valid, the packet is discarded. Infoblox recommends that some form of RPF be implemented in the network to help reduce spoofed traffic. See BCP-38, BCP-84

Holddown / fetches_per_server / fetches_per_zone

NIOS provides a few CLI commands for mitigating phantom domain attacks in which a flood of queries are sent to resolve non-existent domains. Under normal circumstances, the DNS recursive server contacts authoritative servers to resolve recursive queries. When phantom domain attacks happen, the recursive server continues to query non-responsive servers. To mitigate phantom domain attacks, the following commands should be enabled to control queries to non-responsive servers:

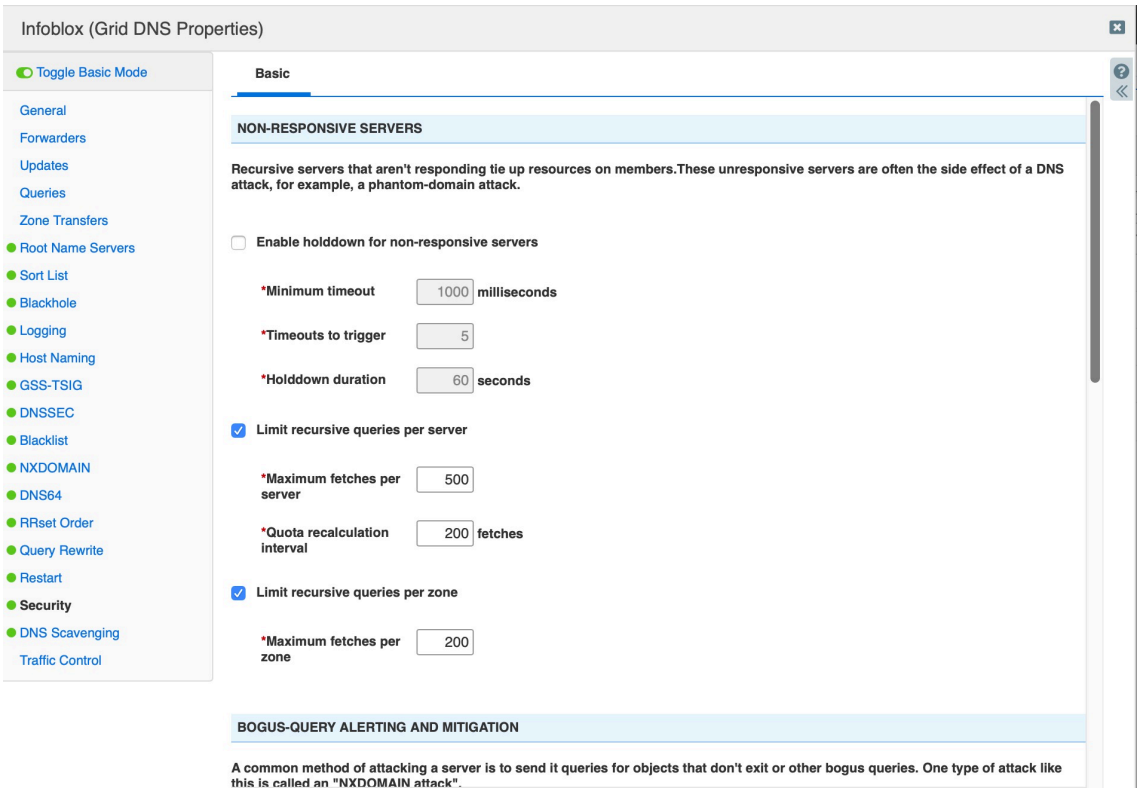
- **`set holddown on (default values:  time: 60s threshold: 5  timeout: 1000ms)`**
- **`set fetches_per_server on (default values:Fetches per server: 500  Frequency: 200)`**
- **`set fetches_per_zone on (200)`**

Definitions:
fetches_per_server: The maximum number of concurrent recursive queries that the appliance sends to a single upstream name server. Queries above the limit will be blocked and may result in a SERVFAIL response to the client. When you enable this option, the appliance dynamically adjusts the concurrent query limit for a specific server based on the average timeout ratio (ATR). The SERVFAIL response may be counted against the client by rule 200000003. This may also help reduce the load on an upstream server that may be under attack.

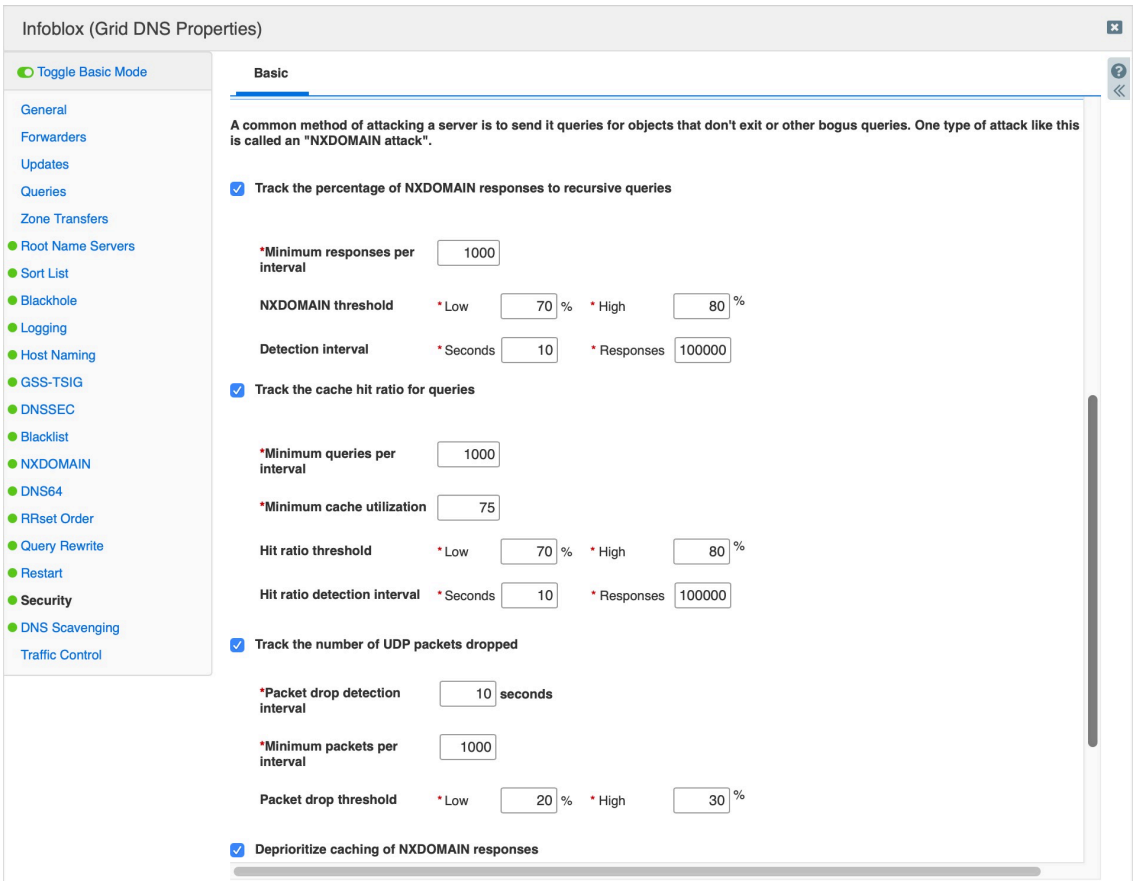
fetches_per_zone: The maximum number of recursive queries the DNS server sends to a domain. If the number of recursive queries exceeds the configured value, the server blocks new queries to that domain and returns a SERVFAIL response to the client. This limit is applied to outstanding (inflight) fetches.

holddown: This will ignore non-responsive servers for a specified time interval. You can use this command to specify the threshold value (the number of consecutive timeouts before holding down a server). When the number of consecutive attempts to contact a non-responsive server exceeds the threshold value, the appliance stops sending queries to the non-responsive servers. This is good for certain type of attacks, but it's being depreciated in favor of fetches_per_server

Below are these features from the GUI at Data Management -> DNS -> Grid DNS Properties (toolbar) -> Security



There are also tunable parameters to reduce the effect of NXdomain attacks



Ruleset Categories

BFD

Auto rules used in conjunction with BGP to support Bidirectional Forwarding Detection.

BGP

Auto rules required to support your member being part of an Anycast deployment.
Provides protection for BGP attacks.

BLACKLIST DROP TCP IP prior to rate limiting

This is one location to drop traffic based on IP, the other place that allow to sinkhole traffic are the dns blackhole feature and RPZ. If you are seeing spoofed incoming traffic from your networks it is advisable to review your network's compliance with BCP 38

BLACKLIST DROP UDP IP prior to rate limiting

This is one location to drop traffic based on IP, the other place that allow to sinkhole traffic are the dns blackhole feature and RPZ. If you are seeing spoofed incoming traffic from your networks it is advisable to review your network's compliance with BCP 38

BLACKLIST DROP UDP FQDN

The following domains can be considered candidates for custom rules, these are domains that are frequently generating a lot of traffic by misconfigured clients. They are also the reverse zones for internal networks which can generate a lot of NXDOMAIN responses :

- .wpad
- .local
- .localdomain
- 1.0.0.127.in-addr.arpa
- 168.192.in-addr.arpa
- 10.in-addr.arpa
- 172.16.in-addr.arpa

DNS Cache Poisoning

In order to be susceptible to this we need to sustain large volumes of dns responses over extended periods of time.

DNS Message Type

These rules will be applied after all the rate limiting, protocol anomalies, … They are the default passes for regular query types.

If you disable this category, you will drop **any** dns query. This a bad idea. **DO NOT DO THIS!**

You can, after very careful consideration, block a single record type by disabling a single rule in this category

General DDoS

This category is meant to prevent a number of classic DDoS techniques

Reconnaissance

A minor category that prevents attackers from fingerprinting the version and author of BIND.

DNS Malware

A list of categories that is dynamically updated with known malware domains. It also includes tor proxies and at the moment of writing over 800 entries. Enabling this category can generate a lot of logging depending on the type of clients that resolve dns through ADP. Having it enabled stops the proliferation of malware in the connected networks as clients cannot connect to their command and control servers anymore.

DNS Protocol Anomalies

Designed to detect and stop invalid DNS traffic and DNS data noncompliant with the standards. While this filters out misbehaving clients you can also see certain IoT devices causing hits because of non-standard DNS behavior.

Potential DDoS Related Domains

Updated list with top DDoS domains being used.

TCP/UDP Flood

These are high in the order of rules and can serve as warning and rate limit rules for DNS traffic. Because they are so high in the order they will limit any lower ordered DNS based rule.

DNS DDoS

As stated in Advanced Rule Tuning. There are a number of rules which take into account the response to the query from each client and will block the offending client entirely from making any more dns queries during the drop interval. You can have internal forward and reverse zones trigger these rules due to common misconfiguration. If the end hosts in your environment cannot be changed to prevent hitting this zone it has to be noted that when you whitelist those zones the response for those zones are not included in the count for these rules.

This makes it possible that you are passing on a high load of NXDOMAIN and SERVFAIL handling load onto the BIND engine.

DNS Tunneling

Category that can detect dns tunnels based on volumetric parameters, this is not to be confused with the Threat Insight product which performs live analysis of traffic.

DNS Amplification and Reflection

This auto rule should in general not be increased over 5 PPS as this allows classic amplification attacks. This is the ANY request it is only used for troubleshooting purposes and should not exceed 1 PPS since only a human should be issuing this request.

The rules with regards to root request can also be brought back to very low values as these requests are in general not encountered by regular dns clients.

NTP

Rules designed to protect ntpd when it is running on your appliance or to discard any ntp traffic when it is not. ADP manages the state of these rules to match the service being enabled or not.

OSPF

Auto rules required to support your member being part of an Anycast deployment.

Provides protection for OSPF attacks. ADP manages the state of these rules to match the service being enabled or not.

ICMP

A category to deal with floods and unexpected ICMP messages.

DHCP

The category protects the dhcp process when it is running on the appliance, in general it is advised not to have any network devices on the same broadcast domain as your ADP appliance. Rules are intended to protect against malicious clients that flood with abnormal amounts of data or with malformed dhcp requests. ADP manages the state of these rules to match the service being enabled or not.

Default Pass/Drop

Generic PASS and DROP rules that are either at the top of the chain or at the bottom to deal with unexpected protocols or

HA Support

Category required to support and protect ADP appliances in HA configurations. ADP manages the state of these rules to match the service being enabled or not.

Custom Rule Templates

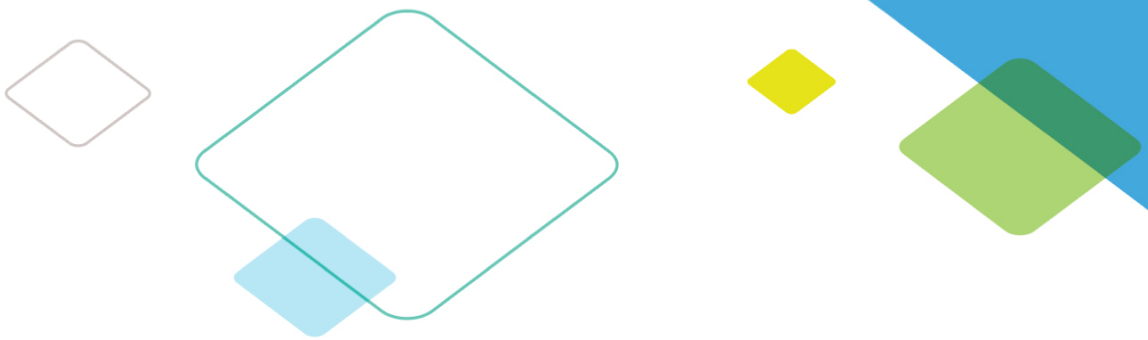
Templates to allow you to specify your whitelists and blacklists. Once a rule is created using these templates it is high in the order of rules that get processed. Adding domains and ip's to these lists will have an impact on the further analysis of the traffic.

Rate Limiting Rules

Identical to Custom Rules, however capable of rate limiting traffic as per ADP actions, Rate limiting.

Additional Documentation

Infoblox Threat Protection Rules - NIOS 8.4 (under Technical Documentation on support site)
- Community Blog
- Relevant API functions
  - WAPI
    - grid:threatprotection
- Admin guide
- DCA admin guide
- ADP initial deployment Guide



Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com