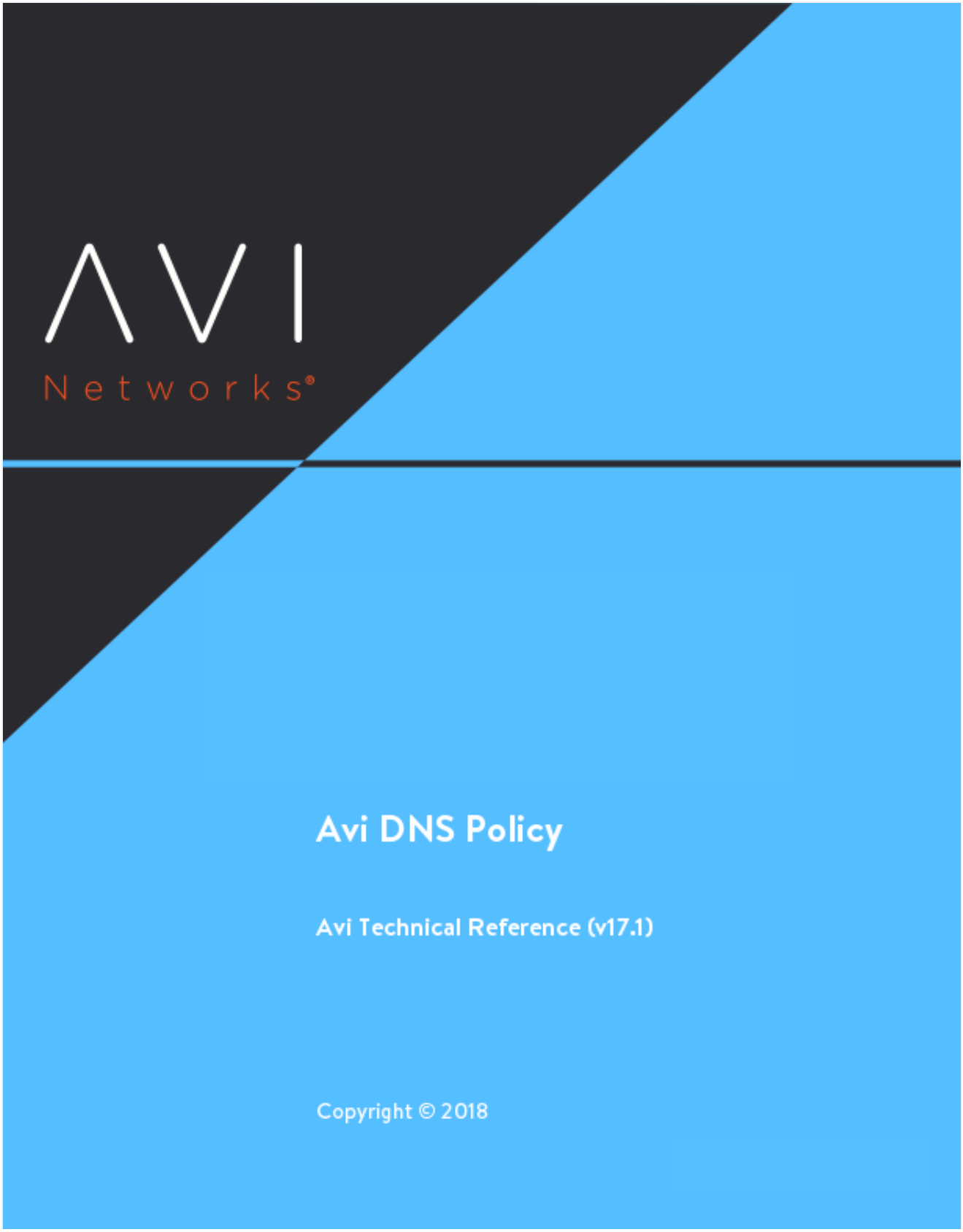


Avi DNS Policy

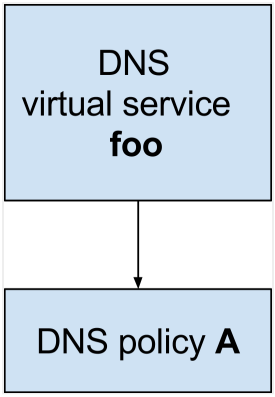
Avi Technical Reference (v17.1)

Avi DNS Policy

view online

A DNS policy consists of rules which in turn consist of match targets and actions. The match targets are the various attributes of a DNS request, such as query type, query domain name, DNS transport protocol used, client IP originating the request, etc. The rule actions can vary from security actions, such as closing the connection, to response actions, such as generating an empty response, etc.

A DNS policy can be referenced by a Layer-4 DNS virtual service (L4 DNS VS) i.e., a virtual service which has an application profile of type DNS. As shown below, a single DNS VS can refer to a single DNS policy.



The DNS rule engine is executed for a DNS request only when a DNS request has been received and parsed successfully.

A DNS policy rule is said to be a hit for a DNS request if all the match targets of the rule evaluate to TRUE. If any match target of the rule does not evaluate to TRUE, then the rule is not considered a hit and the subsequent rule of the current policy (or, if there are no more rules in current policy, then the first rule of the next policy) is evaluated.

> *Note: For a DNS query, the DNS policy rules are applied first, before lookups into the database for GSLB and static DNS entries.*

Rule matching in the DNS policy consists of the following match targets and actions.

Matches

1. Client IP

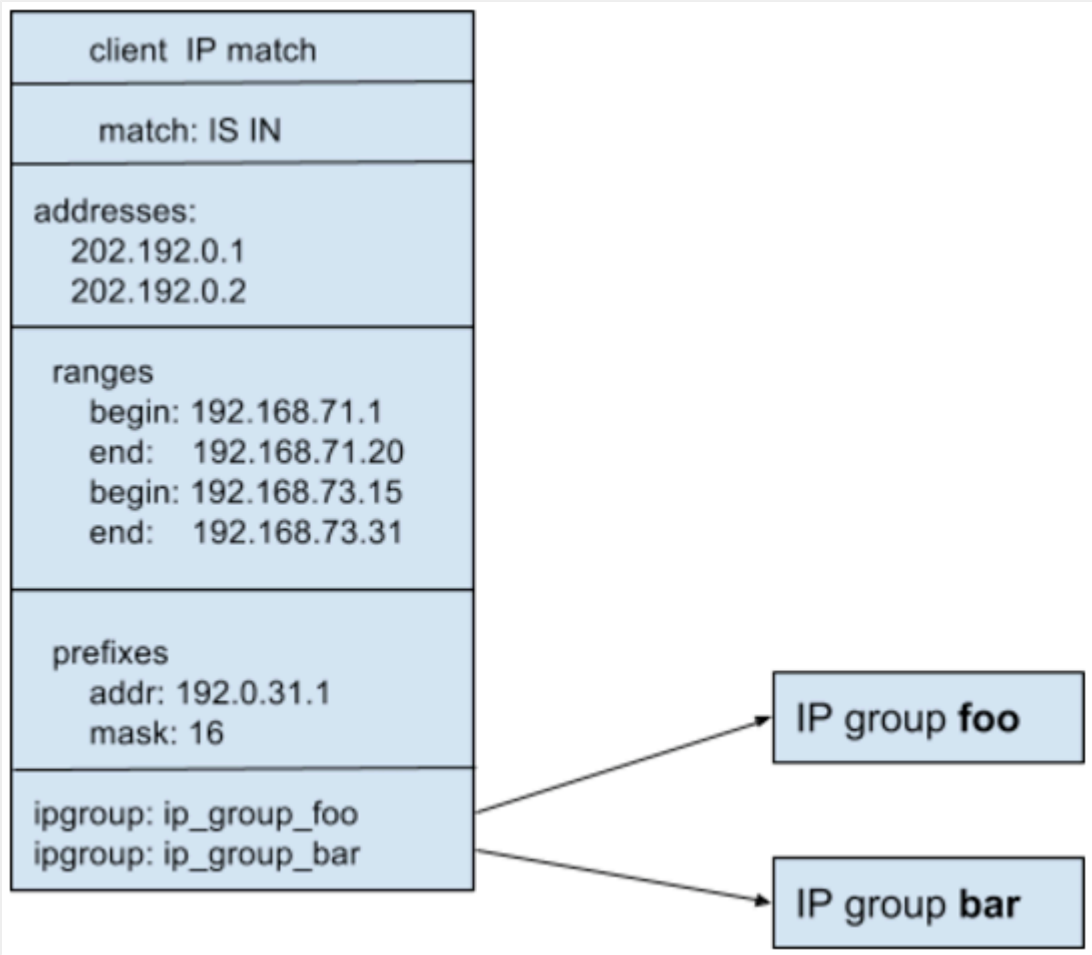
This match target matches the client IP address of the DNS query against a configured set of IP addresses. The IP address match can be against an implicit set of IP addresses, IP address ranges and IP prefixes, and/or a set of IP address group objects.

The client IP match operation supports the following match operations:

- Is In evaluates to TRUE if the client IP of the current DNS request is in the configured set of IP addresses.
- Is Not In evaluates to TRUE if the client IP of the current DNS request is not in the configured set of IP addresses.

Use case

A client IP match target can be used to block DNS queries emanating from a particular geographical area hosting a bad bot. This is achieved by simply configuring a client IP rule match using the IP addresses associated with the particular geographical area, and a rule action of drop (see below).



2. Query Domain Name

This match target matches the query domain name in the DNS query request against the configured set of strings. The query domain name match target supports an implicit set of domain names as match targets as well a set of string group objects.

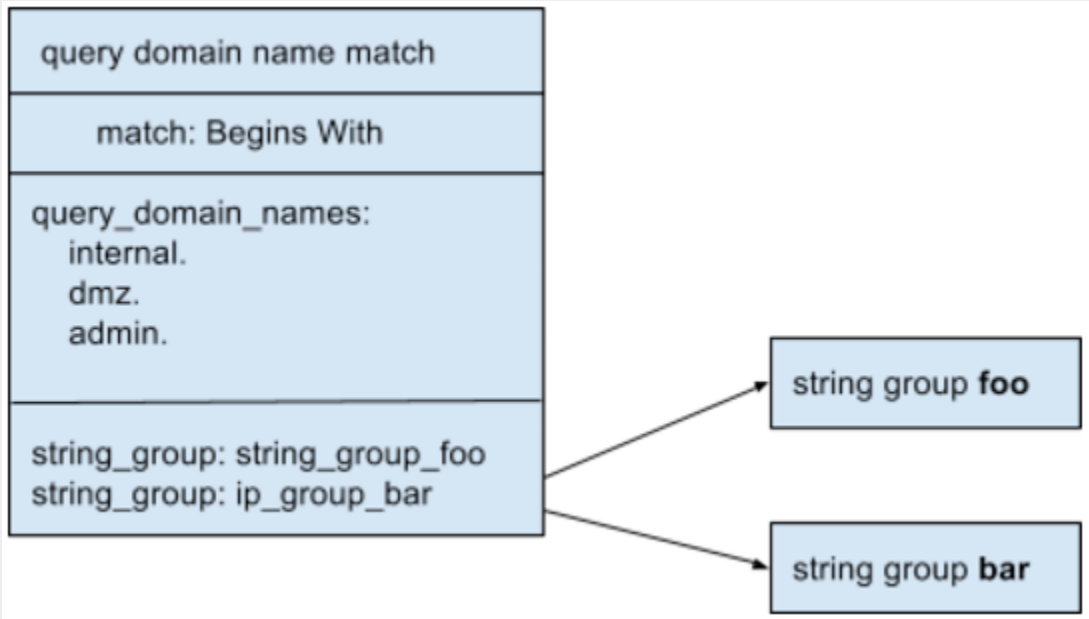
The query name match operation supports the following match operations:

- Begins With evaluates to TRUE if the query domain name of the current DNS request begins with any of the strings in the configured set of strings.
- Does Not Begin With evaluates to TRUE if the query domain name of the current DNS request does not begin with any of the strings in the configured set of strings.
- Contains evaluates to TRUE if the query domain name of the current DNS request contains any of the strings in the configured set of strings.

- Does Not Contain evaluates to TRUE if the query domain name of the current DNS request contains none of the strings in the configured set of strings.
- Ends evaluates to TRUE if the query domain name of the current DNS request ends with any of the strings in the configured set of strings.
- Does Not End With evaluates to TRUE if the query domain name of the current DNS request does not end with any of the strings in the configured set of strings.
- Equals evaluates to TRUE if the query domain name of the current DNS request equals any of the strings in the configured set of strings.
- Does Not Equal evaluates to TRUE if the query domain name of the current DNS request equals none of the strings in the configured set of strings.

Use case

A query domain name match target can be used to block DNS queries for certain domains not served by the DNS VS. This is achieved by simply configuring a rule with query domain name match using the desired unavailable domain names, and a rule action of drop (see below).



3. Query Type

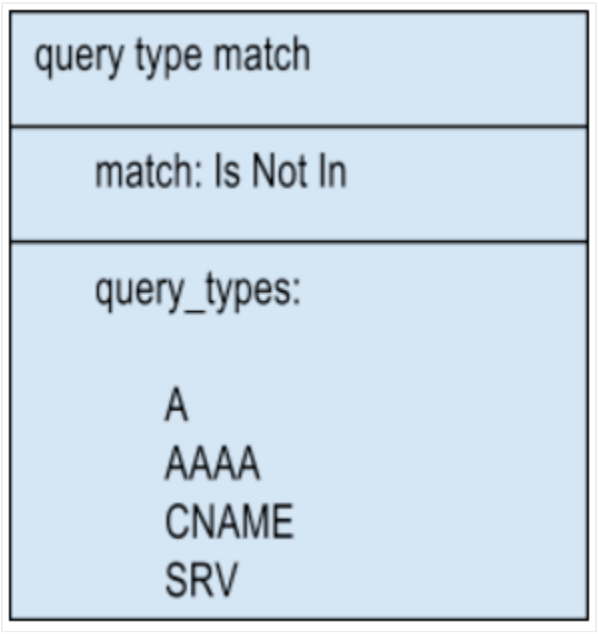
This match target matches the type of the DNS query against a configured set of query types (record types A, AAAA, CNAME, etc.). The query type match operation supports the following match operations:

a. Is In evaluates to TRUE if the query type of the current DNS request is in the configured set of query types.

b. Is Not In evaluates to TRUE if the query type of the current DNS request is not in the configured set of query types.

Use case

A query type match target can be used to block DNS queries not served by the DNS VS. This is achieved by simply configuring a rule query type match using the desired available query types, and a rule action of drop (see below). Thus, any query type not in the configured set will be dropped.



4. DNS Transport Protocol

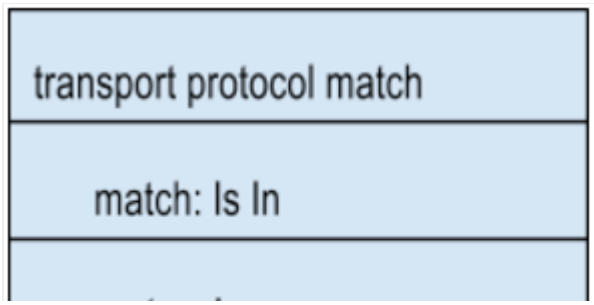
This match target matches the transport protocol carrying DNS query against configured set of transport protocols.

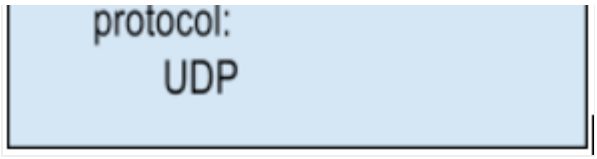
The query type match operation supports the following match operations:

- Is In evaluates to TRUE if the transport of the current DNS request is in the configured set of transport protocols.
- Is Not In evaluates to TRUE if the transport of the current DNS request is not in the configured set of transport protocols.

Use Case

A query transport protocol match target can be used to redirect DNS queries over UDP to instead come over TCP. This is achieved by simply configuring a rule with transport protocol match using the UDP protocol as match, and a rule action of Empty Response with truncation TC bit set (see below). Thus, any query over UDP will receive an empty response with truncation TC bit set, leading the client to retransmit the query over TCP.





Actions

1. Access Control

This rule action allows a UDP DNS query to be processed or dropped. If the query arrives over TCP, it will be allowed or dropped, with the additional option of resetting the connection.

Use Case

If a rule match is configured to block DNS queries of types other than A, AAAA, CNAME and SRV, the drop action is used in the rule.

2. Custom Response

This action allows an empty response to be sent for a DNS query request. The response can be controlled to set the response code RCODE, the Authority AA and Truncation TC bit in the response.

Use case

If the DNS entries in the DNS VS do not support AAAA records for IPv6 address and would like to hint that the client ask for A records, then a rule match is configured to catch AAAA DNS queries, and the response action is used in the rule action to generate an empty NOERROR response, causing the client to reissue the query for an A record.

3. GSLB Site Selection (as of 17.1.5)

The DNS VS's policy is configured so that a rule match may override the usual GSLB-algorithm-based response. As a result of a match, one site is chosen from a set of IP addresses (each homed at a different GSLB site) that share a common `site_name` tag. If none of these are available, up to 16 *fallback* sites may be identified as an alternative. If none of the fallback sites are healthy, and the `is_preferred_site` Boolean is True, the DNS VS picks a site based on the configured GSLB algorithm. Read more.

Use case

Imagine three GSLB sites, one in Paris, one in Lyons, and one in Antwerp. With Avi's geolocation algorithm in play, a client situated in France, close to the French-Belgian border would normally be directed to Antwerp. However, since the client is in France, the GSLB-site-selection action instead returns the VIP of a site having the site name "FRANCE."

