DNS Type Query Support Added to the DNS Analyzer

This chapter describes the following topics:

- Feature Summary and Revision History, on page 1
- Feature Changes, on page 2
- Command Changes, on page 4
- Performance Indicator Changes, on page 5

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ECS
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *ECS Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
In this release, the DNS analyzer (ECS) is enhanced to query the DNS type. This capability supports zero-rating on A type of queries and DNS tunneling on TXT and NULL type queries.	21.4
First introduced.	Pre 21.2

Feature Changes

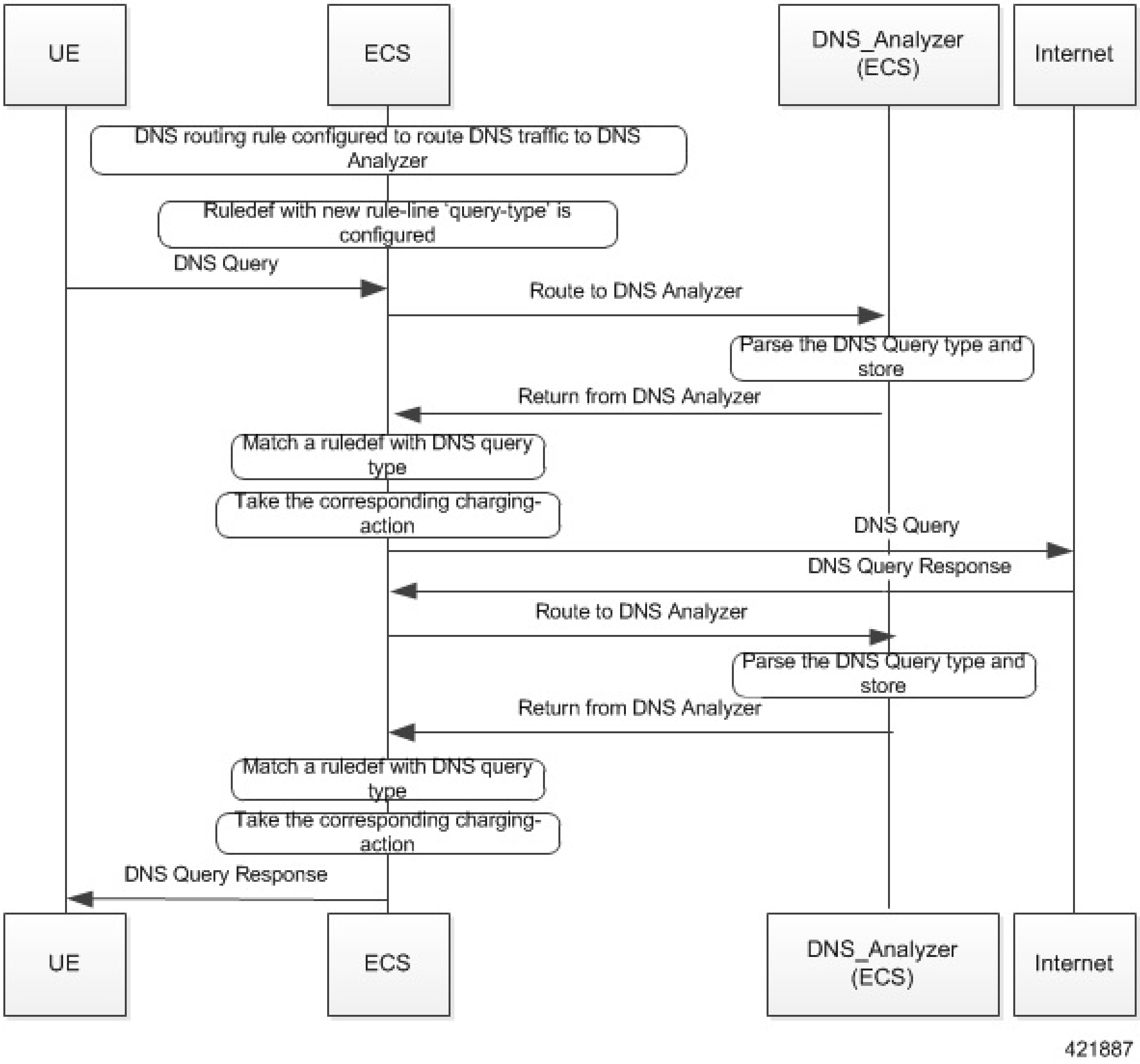
The DNS analyzer currently does not detect the type of DNS query nor does it perform zero-rating on A type DNS queries.

The new command **dns query-type** is introduced to enable the DNS analyzer (ECS) to query the DNS type to counter DNS fraud without huge impacts. This capability supports zero-rating on A type of queries and DNS tunneling on TXT and NULL type queries.

The Rule Match engine is enabled to support matching based on the query type.

The **dns query-type** command defines rule expressions to match the query type in the DNS request messages. This command is added under the ACS Ruledef Configuration Mode.

The following call flow displays how the DNS analyzer (ECS) detects the type of DNS query.


UE
ECS
DNS_Analyzer (ECS)
Internet
DNS routing rule configured to route DNS traffic to DNS Analyzer
Ruledef with new rule-line 'query-type' is configured
DNS Query
Route to DNS Analyzer
Parse the DNS Query type and store
Return from DNS Analyzer
Match a ruledef with DNS query type
Take the corresponding charging-action
DNS Query
DNS Query Response
Route to DNS Analyzer
Parse the DNS Query type and store
Return from DNS Analyzer
Match a ruledef with DNS query type
Take the corresponding charging-action
DNS Query Response
UE
ECS
DNS_Analyzer (ECS)
Internet
421887

Previous Behavior

DNS query types based rule-matching never occurred. If there were multiple answers, unsupported query-type skipped parsing the complete answer.

New Behavior

The following DNS query types can be configured in a ruledef. These are parsed and rule-matched.

- A
- CNAME
- NS
- PTR
- SRV

- AAAA
- TXT
- ANY
- NULL

If there are multiple answers, unsupported query-type skips parsing only that answer and continues parsing the next answer.

Customer Impact

DNS packets now start matching the query-type ruledefs.

Command Changes

dns query-type

This new command is added under the ACS Ruledef Configuration mode to define rule expressions to match the query type in the DNS request messages.

When enabled, the **dns query-type** CLI supports the following behavior:

- DNS request with only one query is supported.
- DNS response with multiple answers is supported. Query-type corresponding to all the answers is stored and matched to the highest priority ruledef.
- For DNS response with multiple answers, unsupported query-type (mentioned previously) is skipped and parsing continues for remaining answers.
- For TXT and NULL query types, minimal parsing occurs like only a DNS record is created and query-type is stored. Answer-name is not extracted and hence the corresponding EDR field is not populated.
- For NULL query types, response is not parsed and matching is based on the same ruledef as a Request.

```
configure
    active-charging service  service_name
       ruledef  ruledef_name
        [ no ] dns query-type operator query_type
        end
```

Notes:

- **no**: Disables this feature, that is, the query-name ruleline is removed from the DNS protocol.
- **operator:** Specifies how to match.

  operator must be one of the following:

  - **=**: Specifies that the query-name must be equal to the one specified.
  - **!=**: Specifies that the query-name must not be equal to the one specified.

- **query-type**: Specifies the type of queries supported: a, cname, ns, ptr, srv, aaaa, txt, any, and null.
- This CLI is disabled by default.

Performance Indicator Changes

show active-charging analyzer statistics name dns

The output of this command now includes the following new fields (TXT and NULL query types) depending on whether the CLI is enabled or disabled:

```
show active-charging analyzer statistics name dns
ACS DNS Session Stats:
  Total Uplink Bytes:               0   Total Downlink Bytes:              0
  Total Uplink Pkts:                 0   Total Downlink Pkts:                0
  Unknown OPCODE:             0   Invalid Pkts:                              0

  DNS Over TCP:
    Uplink Bytes:                       0   Downlink Bytes:                     0
    Uplink Pkts:                         0   Downlink Pkts:                        0

  Request:
    A Query Type:                     0   CNAME Query Type:              0
    NS Query Type:                   0   PTR Query Type:                     0
    SRV Query Type:                0   Unknown Query Type:             0
    AAAA Query Type:            0    TXT Query Type:                    0
    NULL Query Type:             0
  Response:
    A Query Type:                     0   CNAME Query Type:               0
    NS Query Type:                   0   PTR Query Type:                      0
    SRV Query Type:                0   Unknown Query Type:              0
    AAAA Query Type:            0    TXT Query Type:                    0
    NULL Query Type:              0
```

Bulk Statistics

This section lists all the bulk statistics that have been added, modified, or deprecated to support this feature.

ECS Schema

This section displays the new bulk stats that are collected for the new query types:

- dns-req-txt-query—Indicates the number of DNS queries with 'TXT' query type.
- dns-rsp-txt-query—Indicates the number of DNS answers with 'TXT' query type.
- dns-req-null-query—Indicates the number of DNS queries with 'NULL' query type.
- dns-rsp-null-query—Indicates the number of DNS answers with 'NULL' query-type.