Troubleshoot Secure Web Appliance DNS Service

Contents

Introduction

This document describes Domain Name Service (DNS) configuration and how to troubleshoot in Secure Web Appliance(SWA) formerly known as WSA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Physical or Virtual Secure Web Appliance (SWA) Installed
- License activated or installed
- Secure Shell (SSH) Client
- The setup wizard completed

- Administrative Access to the SWA

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

DNS Concept

DNS is the system in the Internet that maps names of objects (usually host names) into Internet Protocol (IP)

address or other resource record values.

The name space of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain.

The domain name space is divided into areas called zones that are points of delegation in the DNS tree.

A zone contains all domains from a certain point downward, except those for which other zones are authoritative.

A zone usually has an authoritative name server, often more than one.

In an organization, you can have many name servers, but Internet clients can query only those that the root name servers know.

The other name servers answer internal queries only.

DNS is based on a client/server model. In this model, name servers store data about a portion of the DNS database and provide it to clients that query the name server across the network.

Name servers are programs that run on a physical host and store zone data. As administrator for a domain, you set up a name server with the database of all the Resource Records (RRs) describing the hosts in your zone or zones

DNS Service in Proxy Deployments

In the **Explicit** Deployment: The proxy runs DNS queries

In the **Transparent** Deployment: DNS queries runs on the client.

Configure DNS Settings

You can Configure DNS from both Graphical User Interface (GUI) and Command Line Interface (CLI).

AsyncOS for Web can use the Internet root DNS servers or your own DNS servers. If SWA use Internet root servers, you can specify alternate servers to use for specific domains.

Since an alternate DNS server applies to a single domain, it must be authoritative (provide definitive DNS records) for that domain.

AsyncOS supports split DNS where internal servers are configured for specific domains and external or root DNS servers are configured for other domains.

If SWA use on premise DNS server, we can also specify exception domains and associated DNS server.

Best Practice

Security best practices suggest that every network must host two DNS resolvers: one for authoritative records from within a local domain, and one for recursive resolution of Internet domains.

To accommodate this, the SWA allows DNS servers to be configured for specific domains.

In the case of one DNS server available for both local and recursive queries, consider the additional load this would add if it is used for all SWA queries.

The better option can be to use the internal resolver for local domains and the root Internet resolvers for external domains. This is dependent on the administrator risk profile and tolerance.

Secondary DNS servers must be configured in case the primary is not available. If all servers are configured with the same priority, the server IP would be chosen at random.

Depending on the number of servers configured, the timeout for a given server is vary. The timeout for a query is given in this table, for up to six DNS servers:

Number of DNS servers	Query timeout (in sequence)
1	60
2	5, 45
3	5, 10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

For more information visit : Cisco Web Security Appliance Best Practices Guidelines - Cisco

Configure DNS in GUI

To configure DNS from GUI, use these steps:

Step 1. Choose **Network** from Top Menu

Step 2. Choose **DNS**

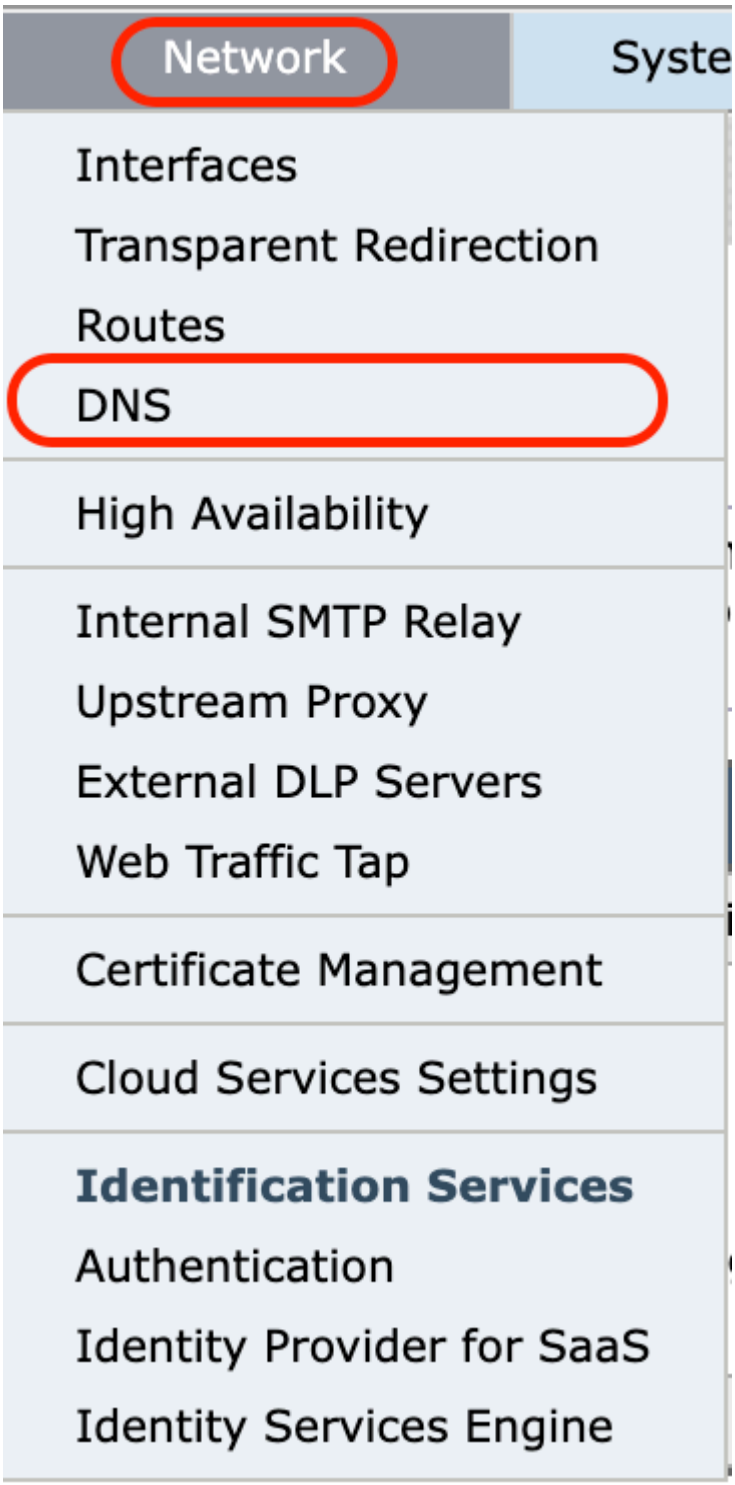

Image-GUI - Configure DNS settings

Step 3. Select **Edit Settings**.
Step 4. Configure the DNS settings as required.

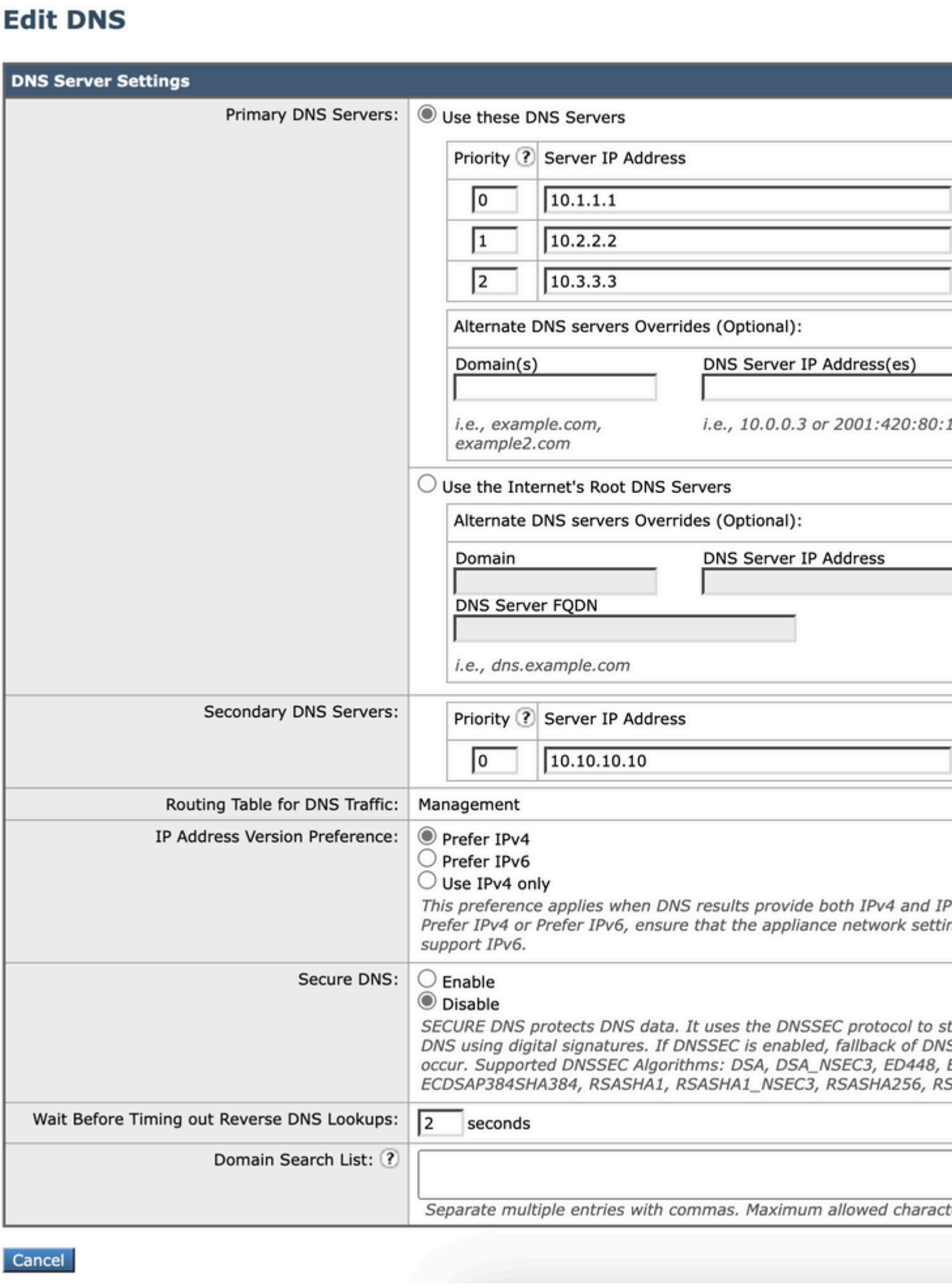

Image - DNS configuration

Use these DNS Servers: The local DNS server(s) that the appliance can use to resolve hostnames

Alternate DNS servers Overrides (Optional): Authoritative DNS servers for domains

---

Note: AsyncOS does not honor the version preference for transparent FTP requests.

Note: In Cloud Connector mode, Cisco Web Security Appliance supports IPv4 only

---

Use the Internet Root DNS Servers. Choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network.

Internet Root DNS servers do not resolve local hostnames.

Note: If you need your appliance to resolve local hostnames, use a local DNS server or add the appropriate static entries to the local DNS from the Command Line Interface (CLI).

Domain Search List: A DNS domain search list used when a request is sent to a bare hostname (with no dot " . ").

The domains specified each be attempted in turn, in the order entered (Left to Right), to see if a DNS match for the hostname plus domain can be found.

Routing Table for DNS Traffic: Specifies which interface the DNS service route the traffic through.

Wait Before Timing out Reverse DNS Lookups: The wait time in **seconds** before time out non-responsive reverse DNS lookups.

The secondary DNS servers receive host name queries when the primary DNS servers return these errors:

- â€¢ No Error, no answer section received
- â€¢ Server failed to complete request, no answer section
- â€¢ Name Error, no answer section received
- â€¢ Function not implemented
- â€¢ Server Refused to Answer Query

Note: AsyncOS evaluates transactions based on policies before it evaluates external dependencies to avoid unnecessary external communication from the appliance. For example, if a transaction is blocked based on a policy that blocks un-categorized URLs, the transaction would not fail based on a DNS error.

Priority: A value of 0 has the highest priority. A random IP is selected if both have the same priority.

Configure DNS from CLI

You can use **dnsconfig** from CLI to configure DNS settings.

Step1. Type **dnsconfig** in CLI:

```
SWA_CLI> dnsconfig
```

```
Currently using the local DNS cache servers:
1. Priority: 0  10.1.1.1
2. Priority: 1  10.2.2.2
3. Priority: 2  10.3.3.3

Currently using the following Secondary DNS cache servers :
1. Priority: 0  10.10.10.10

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]>
```

Step 2. To add a new DNS server to the list, type NEW and press Enter.

Step 3. Choose between Primary DNS nameservers or Secondary DNS nameservers, to which you want to add a new nameserver.

```
[]> NEW

Do you want to make changes in the Primary DNS nameserver list or secondary DNS nameserver list?
1. Make changes to the primary DNS nameserver
2. Make changes to the secondary DNS nameserver
[]> 1
```

Step 4. Choose to add a new name server or an alternate domain server (conditional forwarding Domain Name)

```
Do you want to add a new local DNS cache server or an alternate domain server?
1. Add a new local DNS cache server.
2. Add a new alternate domain server.
[]> 1
```

Step 5. Provide the IP address of the new name server

Step 6. Provide the priority for the newly added name server.

```
Please enter the IP address of your DNS server.
Separate multiple IPs with commas.
[]> 10.4.4.4

Please enter the priority for 10.4.4.4.
A value of 0 has the highest priority.
The IP will be chosen at random if they have the same priority.

[0]> 4
```

```
Currently using the local DNS cache servers:
1. Priority: 0  10.1.1.1
2. Priority: 1  10.2.2.2
3. Priority: 2  10.3.3.3
4. Priority: 4  10.4.4.4

Currently using the following Secondary DNS cache servers :
1. Priority: 0  10.10.10.10
```

Step 7. Press Enter to exit the wizard.

Step 8. Type **commit** to save the changes.

Note: To Edit or Delete any name servers you can choose **EDIT** and **DELETE** from dnsconfig.

From **SETUP** option you can configure the DNS cache time and offline DNS detection settings:

```
SWA_CLI> dnsconfig
....
[]> setup
Do you want the Gateway to use the Internet's root DNS servers or would you like it to use your own DNS
1. Use Internet root DNS servers
2. Use own DNS cache servers
[2]> 2

Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>

Enter the minimum TTL in seconds for DNS cache.
[1800]>

Do you want to enable Secure DNS? [N]> N
Warning: Ensure that you configure the DNS server with DNSSec because there is no backward compatibility
Failing to do so can result in invalid response with an unresolved hostname.

You must use FQDN with the hostname for the local and private domains.

Enter the number of failed attempts before considering a local DNS server offline.
[100]>

Enter the interval in seconds for polling an offline local DNS server.
[5]>
```

Minimum TTL in seconds for DNS cache: This option is to configure the minimum seconds SWA cached a record. for more information visit DNS cache section in this document.

Enter the number of failed attempts before considering a local DNS server offline: If DNS server is not responding to any DNS queries, the counter starts.

When it reaches this defined value, that name server is considered as Offline DNS server and SWA avoids to send the DNS query to that nameserver for a pre-defined time duration (Next option).

When DNS server is marked os offline, you can see this error message:

```
30 Jun 2023 07:37:03 +0200    Reached maximum failures querying DNS server 10.1.1.1
```

Enter the interval in seconds for polling an offline local DNS server: When a DNS server marked as offline, after this time interval (In Seconds), SWA starts to send DNS query to that nameserver and the counter for that DNS server failed reply resets to zero.

CLI DNS Commands

Create Manual Record

To create manual "**A record**" you cannot use or edit Hosts file. You can use **localhosts** hidden command from **dnsconfig** in **CLI.**

> **Note**: You must **commit** changes after changing this configurations.

```
dnsconfig

Currently using the local DNS cache servers:
1. Priority: 0  10.1.1.1
2. Priority: 0  10.2.2.2

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> localhosts

Local IP to Host mappings:

Choose the operation you want to perform:
- NEW - Add new local IP to host mapping.
- DELETE - Delete an existing mapping.
[]> new

Enter the IP address of the host you are adding.
[]> 10.20.30.40

Enter the canonical host name and any additional aliases (separate values
with spaces)
[]> ManualHostEntry.cisco.com
```

dnsflush

dnsflush removes all the cached DNS records from DNS cache table:

```
SWA_CLI> dnsflush
Are you sure you want to clear out the DNS cache? [N]> Y
```

advancedproxyconfig

```
 advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> DNS

Enter values for the DNS options:

Enter the URL format for the HTTP 307 redirection on DNS lookup failure.
[%P://www.%H.com/%u]>

Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?
[Y]>

Would you like proxy not to automatically failover to DNS results when upstream
proxy (peer) is unresponsive?
[N]>

Select one of the following options:
0 = Always use DNS answers in order
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage

For options 1 and 2, DNS will be used if Web Reputation is enabled.
For options 2 and 3, DNS will be used for explicit proxy requests, if there is
no upstream proxy or in the event the configured upstream proxy fails.

For all options, DNS will be used when Destination IP Addresses are used in
policy membership.
Find web server by:
[0]>
```

The HTTP 307 (Temporary Redirect) status code indicates that the target resource resides temporarily under a different Uniform Resource Identifier (URI) and the user agent MUST NOT change the request method if it performs an automatic redirection to that URI. Since the redirection can change over time, the client must continue to use the original effective request URI.

More details on : [What is the HTTP 307 Temporary Redirect Status Code - Kinsta]

These options control how SWA decides on the IP address to connect to, when evaluate a client request in transparent proxy deployment. When a request is received, WSA see a destination IP address and a hostname. SWA must decide whether to trust the original destination IP address for the TCP connection, or to do its own DNS resolution and use the resolved address. The default is**â€œ0 = Always use DNS answers in order,**â€ which means SWA does not trust the client to supply the IP address.

Option 1: SWA tries the client-supplied IP address for the connection, but falls back to the resolved address if that fails. The resolved address is used for policy evaluation (web category, web reputation, and so on).

Option 2: SWA only uses the client-supplied address for the connection and does not fall back. The resolved address is used for policy evaluation (web category, web reputation, and so on).

Option 3: SWA only uses the client-supplied address for the connection and does not fall back. The client-supplied IP address is used for policy evaluation (web category, web reputation, and so on).

The chosen option depends on how much trust the administrator must place in the client when determine the resolved address for a given hostname. If client is a downstream proxy, choose option 3 to avoid the added latency of unnecessary DNS lookups.

DNS cache

To increase efficiency and performance, Cisco SWA stores DNS entries for domains to which you have recently connected. The DNS cache allows SWA to avoid excessive DNS lookups of the same domains. The DNS cache entries expire due to the TTL (Time to Live) of the record.

When the TTL of the record in DNS server is grater than SWA dnsconfig cache TTL time, then dns cache use the TTL from the DNS server.

When the TTL of the record in DNS server is less than SWA dnsconfig cache TTL time, then dns cache use the TTL from WSA dnsconfig setting.

> **Caution**: SWA have two DNS cache, one is designed for Proxy process and the other is used for Internal process.

By default, the SWA cached DNS records for minimum 30 minutes, regardless of the record TTL. Modern websites that make heavy use ofContent Delivery Networks(CDN) would have low TTL records as their IP addresses change frequently.

This could result in a client cache one IP address for a given server and SWA cached a different address for the same server. To counter this, SWA default TTL can be lowered to five minutes from **SETUP** section in **dsnconfig** CLI command.

As an example if the the "**minimum TTL in seconds for DNS cache"** in DNS configuration has been set to 10 minutes and a record has TTL of 5 minutes, the TTL for the cached record increased to 10 minutes.

On the other hand, if the TTL for the record is set to 15 minutes, SWA stores the record for 15 minutes in its cache.

However, it is sometimes necessary to clear the DNS cache of entries. Corrupted or expired DNS cache entries can occasionally cause problems with delivery to a remote host or hosts.

This problem typically occurs after the appliance has been offline for a network move or some other circumstance.

Clear the DNS Cache from GUI

Step 1. Choose **Network** from Top Menu

Step 2. Choose **DNS**

Step 3. Choose **Clear DNS Cache**

> **Caution**: This command can cause a temporary performance degradation while the cache is repopulated

---

Clear the DNS Cache from CLI

The DNS cache in the Cisco WSA can be cleared by **dnsflush**command from the CLI.

View DNS Cache

There is no option to view cached DNS record in SWA from CLI or GUI.

> **Note**: You can not query DNS cache via **nslookup**.

Troubleshoot DNS

View DNS logs

Some log types related to the web proxy component are not enabled. The main web proxy log type, called the â€œDefault Proxy Logs,â€ is enabled by default and captures basic information on all Web Proxy modules.

Each Web Proxy module also has its own log type that you can manually enable as required.

System Logs, Records DNS, error, and commit activity. which is enabled by default

---

> **Tip**: If you change the Log Level for System Logs to DEBUG, you can see the DNS queries and responses.You can change the log level from GUI and CLI.

Change System Logs Log Level from GUI

Step 1. Choose **System Administrations** from Top Menu

Step 2. Choose **Log Subscriptions**

Step 3. Choose **System Logs**

Step 4. Choose **DEBUG** in Log Level section

Step 5. Submit

Step 6. Commit changes

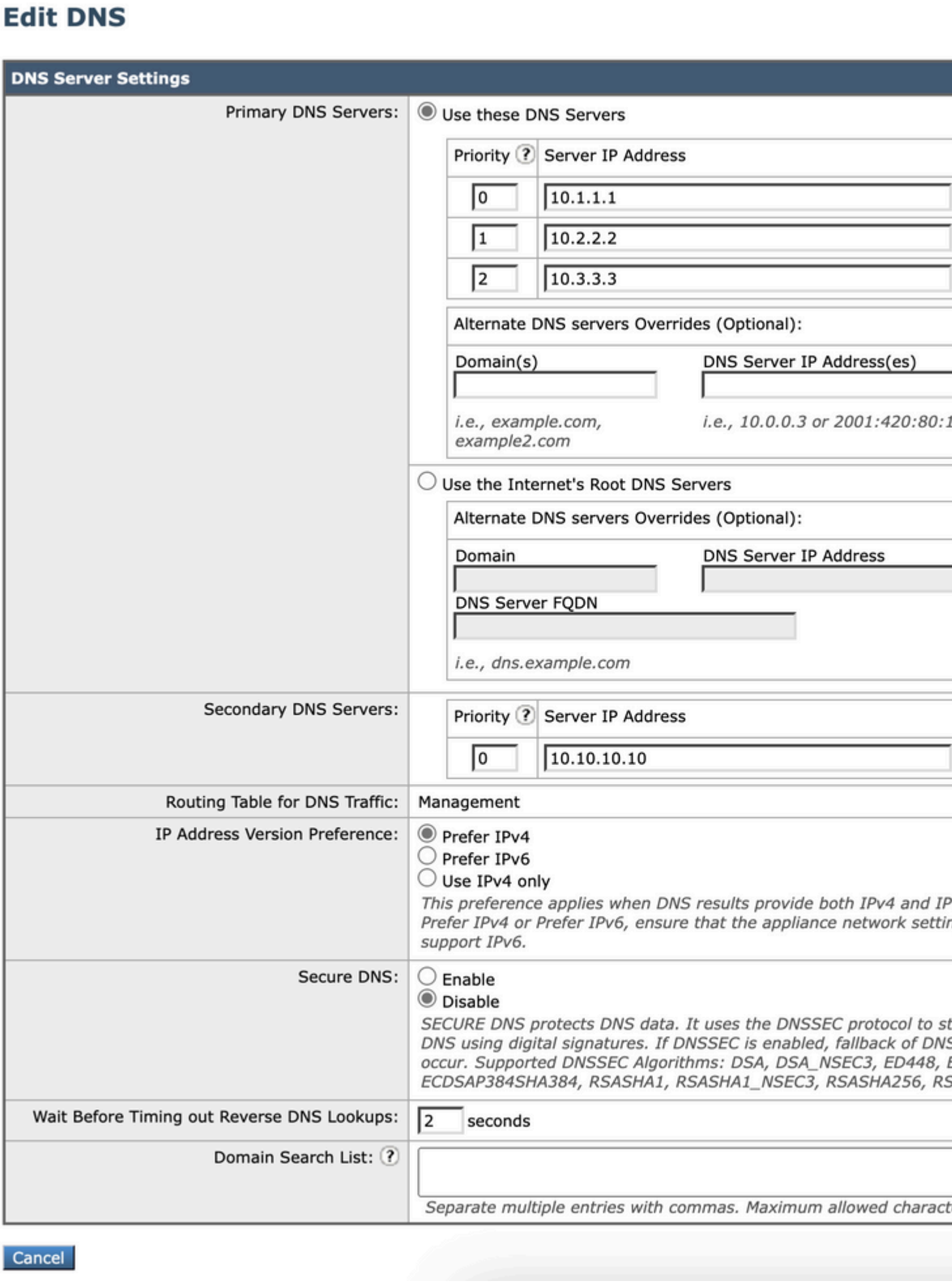

Image - Change System Logs, Log level

Change System Logs Log Level from CLI

, otherwise there would be a huge load on the disk Input / Output (I/O) and the log file would be populated to fast.

nslookup

Use **nslookup** command to see the name resolution response in SWA for different FQDNs.

In this example, in the first attempt to resolve the name the TTL is set to 30 minutes.

On the second attempt, we can see the TTL is less than 30 minutes which indicates that this record was resolved from cache.

```
SWA_CLI> nslookup

Please enter the host or IP address to resolve.
[]> cisco.com

Choose the query type:
1. A       the host's IP address
2. AAAA    the host's IPv6 address
3. CNAME   the canonical name for an alias
4. MX      the mail exchanger
5. NS      the name server for the named zone
6. PTR     the hostname if the query is an Internet address,

 otherwise the pointer to other information
7. SOA     the domain's "start-of-authority" information
8. TXT     the text information
[1]> 1

A=10.20.3.15 TTL=30m

TSWA_CLI> nslookup

Please enter the host or IP address to resolve.
[]> cisco.com

Choose the query type:
1. A       the host's IP address
2. AAAA    the host's IPv6 address
3. CNAME   the canonical name for an alias
4. MX      the mail exchanger
5. NS      the name server for the named zone
6. PTR     the hostname if the query is an Internet address,

 otherwise the pointer to other information
7. SOA     the domain's "start-of-authority" information
8. TXT     the text information
[1]> 1

A=10.20.3.15 TTL=28m 49s
```

dig

dig is another useful command to query the DNS records. With dig you can specify the source interface or

the DNS server in which we want to query:

In this example, here is the query for A-Record from server 10.1.1.1

```
 dig @10.1.1.1 www.cisco.com A


; <<>> DiG 9.16.8 <<>> @10.1.1.1 www.cisco.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58012
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 2cbc212c0877096701000000623db99b050bda7f896790e3 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; ANSWER SECTION:
www.cisco.com.          3600    IN      CNAME   origin-www.cisco.com.
www.cisco.com.   5       IN      A       10.20.3.15

;; Query time: 115 msec
;; SERVER: 10.1.1.1#53(10.1.1.1)
;; WHEN: Fri Mar 25 12:46:19 GMT 2022
;; MSG SIZE  rcvd: 111
```

The usage of **dig**:

```
dig [-s <source IP>] [-t] [-x <IP Address>] [@<IP address>] hostname [qtype]

        Query a DNS server.

        @<IP address> - Query the DNS server at this IP address
        hostname - Record that you want to look up.
        qtype - Query type: A, PTR, CNAME, MX, SOA, NS, TXT
    options:
        -s IP Address
            Specify the source IP address.
        -t
            Make query over tcp.
        -x IP Address
            Do a reverse lookup on this IP address.
```

> **Tip**: You can choose source IP to choose from which interface you want to query the name resolution.

Slow DNS Response

If loading all or some URLs took a longer time (compared to when you refresh the same page), it is better to check the DNS response time. There are two options in SWA to check the DNS response time:

- Configure AccessLogs custom feild.
- Trackstat logs.

Modify Accesslogs to View DNS Statistics

You can modify Accesslogs to view DNS time for each web request.

Step 1. Log in to**GUI**.

Step 2. From System Administration menu, choose **Log Subscriptions.**

Step 3. From Log Name column, click **accesslogs,**or the name of the newly created. In this example, TAC_access_logs.

Step 4. In Custom Fields section, paste this string:

```
[DNS response = %:<d, DNS total = %:>d]
```

Step 5.Submit and **commit** changes.

Custom Field Name	Custom Field	W3C Logs	Description
DNS response	%:<d	x-p2p-dns-wait-time	Time taken by the Web Proxy to send the Domain Name Request (DNS) request to the Web Proxy DNS process.
DNS total	%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS process to send back a DNS result to the Web Proxy.

For more information how to edit custom fields in Accesslogs, you can visit this link: Configure Performance Parameter in Access Logs - Cisco

Overal DNS Response Time in Trackstat logs

You can view statistics of DNS service and other internal services in trackstat logs. You can access trackstats logs by connect via FTP to your SWA.

In this example you can see the cache statistics, and number of DNS responses, categorized by time elapsed from DNS server since SWA was last rebooted.

```
...
INFO: DNS Cache Stats: Entries 662, Expire 1697, Hits 88739, Misses 664, Reclaims 0
...
       DNS Time       1.0 ms    349
       DNS Time       1.6 ms    550
       DNS Time       2.5 ms    374
       DNS Time       4.0 ms    32
       DNS Time       6.3 ms    35
       DNS Time      10.0 ms    37
       DNS Time      15.8 ms    301
       DNS Time      25.1 ms    80
       DNS Time      39.8 ms    136
       DNS Time      63.1 ms    91
       DNS Time     100.0 ms    12
       DNS Time     158.5 ms    33
       DNS Time     251.2 ms    14
       DNS Time     398.1 ms    12
       DNS Time     631.0 ms    45
       DNS Time    1000.0 ms    120
       DNS Time    1584.9 ms    73
       DNS Time    2511.9 ms    296
       DNS Time    3981.1 ms    265
       DNS Time    6309.6 ms    190
```

For example, in the last line, it indicates that 190 DNS queries took more than 6,309 milliseconds (approximatly 6 seconds) to finish since SWA was last rebooted.

To find out the exact number in a time period, subtract these values for the start time and end time.

For example, to identify the DNS response time from 10:00 AM to 11:00 AM, collect statistics for 11:00 AM and subtract them from statistics from 10:00 AM.

The result is the DNS response time from 10:00 AM to 11:00 AM for the desired date.

> **Note**: Track stats logs are collected for every 5 minutes.

Packet Capture

You can capture packets to view the DNS requests and responses, to filter just for DNS you can use: **port 53** .

To start packet capture from GUI:

Step 1. Choose **Support and Help** from Top Right

Step 2. Choose **Packet Capture**

Step 3. (Optional) Choose **Edit Settings** to add filter

Step 4. (Optional) Choose your Interface(s) and Type port 53 in the **Custom Filter** Section

Step 5. (Optional) Choose **Submit**

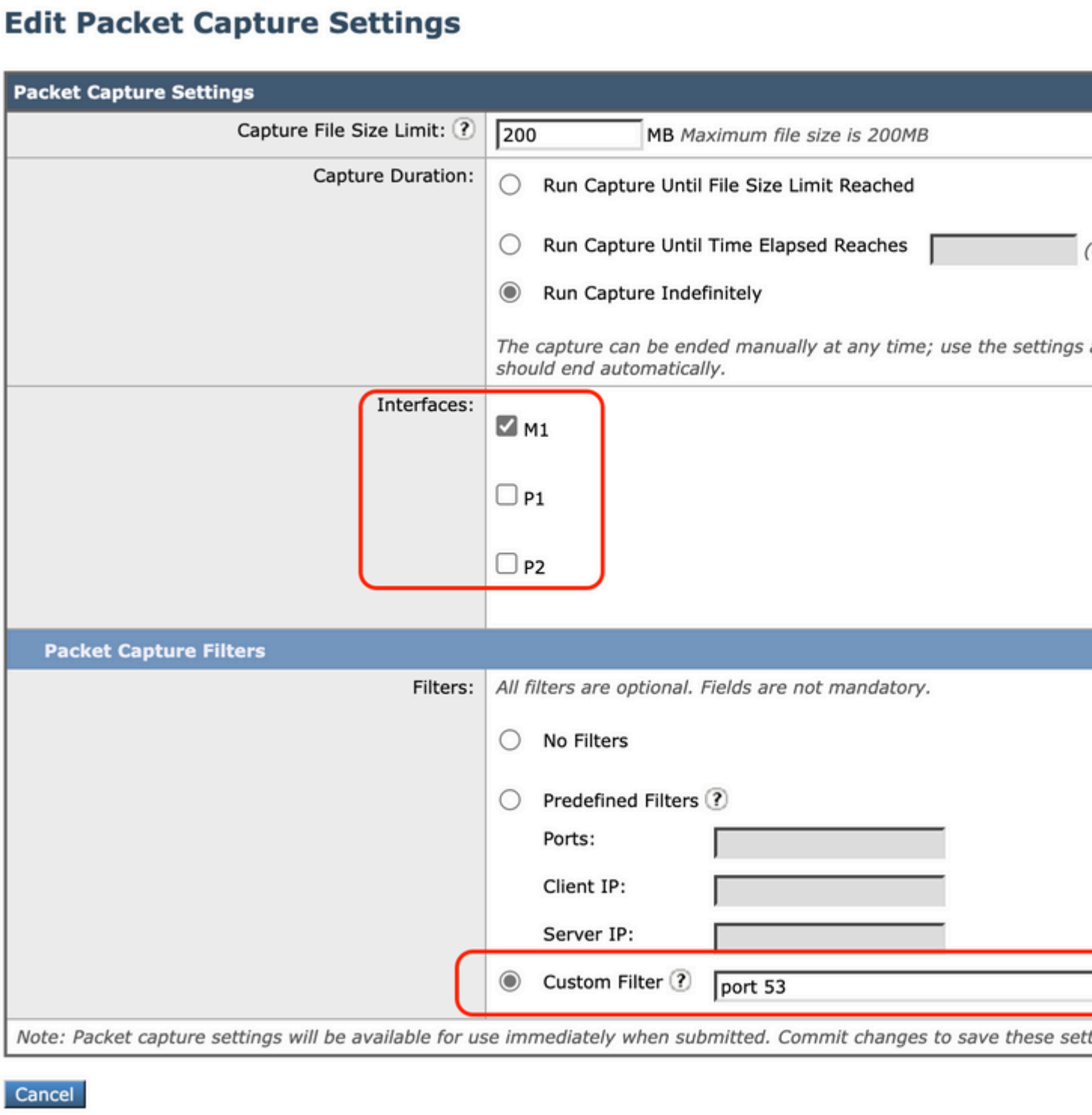

Image- Add Filter To Capture DNS Packets

> **Tip**: Packet capture settings is available to use immediately when submitted. Commit changes to save these settings permanently for future use.

Step 6. Choose **Start Capture**.

Step 7. (Optional) Generate traffic, if you need to trouble shoot specific site or URL access.

Step 8. Stop Capture

Step 9. Wait for the page to refresh, then choose the first packet capture from "**Manage Packet Capture Files**" list

Step 10. Choose **Download File**

? is generated when an appliance is rebooted, it means that the system was unable to contact its primary DNS servers.

This can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not set to a valid server

Reached maximum failures querying DNS server

If one or some of DNS servers configured in SWA, did not reply back to DNS queries, SWA consider them as offline and would not send the DNS queries to them for predefined amount of time. For more information, read "**Configure DNS from CLI**" in this article.

DNS_FAIL

When SWA receives an HTTP request andfailsto resolve the hostname, by default SWA would return a reply like as:

```
GET http://cisco HTTP/1.1
User-Agent: curl/7.19.7 (universal-apple-darwin10.0) libcurl/7.19.7 OpenSSL/0.9.8l zlib/1.2.3
Host: hostname
Accept: */*
Proxy-Connection: Keep-Alive

HTTP/1.1 307 Temporarily Moved for Domain Name Expansion
Mime-Version: 1.0
Date: Wed, 15 Sep 2022 13:05:02 EST
Proxy-Connection: keep-alive
Location: http://www.cisco.com/
Content-Length: 2068
```

This feature is called "**server name expansion**".
WSA does this in attempts that redirected hostname would resolve the expected page for the client.

You can change "URL format for the HTTP 307 redirection on DNS lookup failure", for more information review **advanceproxyconfig** section in this article.

WSA treats DNS request which returns **ServFail** as a failure.
For example, NXDOMAIN would return "DNS_FAIL" instead of "SERVER_NAME_EXPANSION"

Related Information

User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance

Use Secure Web Appliance Best Practices - Cisco

Cisco Content Hub - Introduction to the Domain Name System