

Secure Web Appliance DNSサービスのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[DNSの概念](#)

[プロキシ導入でのDNSサービス](#)

[DNS設定の構成](#)

[ベストプラクティス](#)

[GUIでのDNSの設定](#)

[CLIからのDNSの設定](#)

[CLI DNSコマンド](#)

[手動レコードの作成](#)

[dnsflush](#)

[advancedproxyconfig](#)

[DNS キャッシュ](#)

[GUIからのDNSキャッシュのクリア](#)

はじめに

このドキュメントでは、ドメインネームサービス(DNS)の設定と、以前はWSAと呼ばれていたSecure Web Appliance(SWA)でのトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インストールされている物理または仮想のセキュアWebアプライアンス(SWA)
- ライセンスの有効化またはインストール
- セキュアシェル(SSH)クライアント
- セットアップウィザードが完了しました

- SWAへの管理アクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

DNSの概念

DNSは、オブジェクトの名前(通常はホスト名)をインターネットプロトコル(IP)アドレスまたはその他のリソースレコード値にマッピングするインターネット内のシステムです。

インターネットのネームスペースは、ドメインに分割されており、各ドメイン内でのネームの管理は、通常、各ドメインのシステムに一任されています。

ドメイン名空間は、DNSツリー内の委任ポイントであるゾーンと呼ばれる領域に分割されます。

ゾーンには、他のゾーンが権限を持つドメインを除き、特定のポイントから下方にあるすべてのドメインが含まれます。

ゾーンには通常、権限を持つネームサーバがあり、多くの場合、複数のネームサーバがあります。

組織では、多数のネームサーバを使用できますが、インターネットクライアントが照会できるのは、ルートネームサーバが認識しているネームサーバだけです。

他のネームサーバは、内部クエリーにのみ応答します。

DNSはクライアント/サーバモデルに基づいています。このモデルでは、ネームサーバはDNSデータベースの一部に関するデータを保存し、ネットワーク経由でネームサーバにクエリーを実行するクライアントに提供します。

ネームサーバは、物理ホスト上で実行され、ゾーンデータを格納するプログラムです。ドメインの管理者は、ゾーン内のホストを記述するすべてのリソースレコード(RR)のデータベースを使用してネームサーバーを設定します

プロキシ導入でのDNSサービス

Explicit導入では、プロキシがDNSクエリーを実行します

透過的な導入では、DNSクエリーはクライアントで実行されます。

DNS設定の構成

DNSは、グラフィカルユーザインターフェイス(GUI)とコマンドラインインターフェイス(CLI)の両方から設定できます。

AsyncOS for Webは、インターネットルートDNSサーバまたは独自のDNSサーバを使用できます。SWAがインターネットルートサーバを使用する場合、特定のドメインに対して使用する代替サーバを指定できます。

代替DNSサーバは1つのドメインに適用されるため、そのドメインに対する権限を持つ（正式なDNSレコードを提供する）必要があります。

AsyncOSはスプリットDNSをサポートします。スプリットDNSでは、内部サーバが特定のドメイン用に設定され、外部またはルートDNSサーバが他のドメイン用に設定されます。

SWAがオンプレミスのDNSサーバを使用する場合は、例外ドメインと関連するDNSサーバも指定できます。

ベスト プラクティス

セキュリティのベストプラクティスでは、すべてのネットワークで2つのDNSリゾルバをホストする必要があることを提案しています。1つはローカルドメイン内からの権威レコード用で、もう1つはインターネットドメインの再帰的な解決用です。

これに対応するため、SWAでは特定のドメインに対してDNSサーバを設定できます。

ローカルクエリと再帰クエリの両方に1つのDNSサーバが使用できる場合は、すべてのSWAクエリに使用した場合に追加される負荷を考慮してください。

ローカルドメインには内部リゾルバを使用し、外部ドメインにはルートインターネットリゾルバを使用するのが、より適切なオプションです。これは、管理者のリスクプロファイルと許容範囲によって異なります。

セカンダリDNSサーバは、プライマリが使用できない場合に備えて設定する必要があります。すべてのサーバが同じ優先順位で設定されている場合、サーバIPはランダムに選択されます。

設定されたサーバの数に応じて、特定のサーバのタイムアウトは異なります。最大6台のDNSサーバに対するクエリのタイムアウトを次の表に示します。

DNSサーバの数	クエリのタイムアウト（順序）
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

詳細については、次のサイトを参照してください。[Cisco Webセキュリティアプライアンスのベストプラクティスガイドライン - シスコ](#)

GUIでのDNSの設定

GUIからDNSを設定するには、次の手順を使用します。

ステップ 1 : トップメニューからNetworkを選択します

ステップ 2 : DNSを選択します

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

Web Traffic Tap

Certificate Management

Cloud Services Settings

代替DNSサーバーの上書き (オプション) :ドメインの権限のあるDNSサーバー

 注 : AsyncOSは、トランスペアレントFTP要求のバージョンプリファレンスを承認しません。

 注 : クラウドコネクタモードでは、Cisco WebセキュリティアプライアンスはIPv4のみをサポートします

インターネットルートDNSサーバを使用します。アプライアンスがネットワーク上のDNSサーバにアクセスできない場合に、ドメインネームサービス(DNS)の検索にインターネットルートDNSサーバを使用することを選択します。

インターネットルートDNSサーバは、ローカルホスト名を解決しません。

 注 : アプライアンスでローカルホスト名を解決する必要がある場合は、ローカルDNSサーバを使用するか、コマンドラインインターフェイス(CLI)からローカルDNSに適切なスタティックエントリを追加します。

ドメイン検索リスト : 要求がベアホスト名に送信されるときに使用されるDNSドメイン検索リスト (ドット「」なし) 。 」) を再生します。

指定した各ドメインを順番に (左から右に) 入力した順序で試行し、ホスト名とドメインのDNS一致が見つかるかどうかを確認します。

DNSトラフィックのルーティングテーブル : DNSサービスがトラフィックをルーティングするインターフェイスを指定します。

Wait Before Timing out Reverse DNS Lookups : 応答しない逆DNSルックアップがタイムアウトするまでの待機時間(秒)。

セカンダリDNSサーバは、プライマリDNSサーバが次のエラーを返したときにホスト名クエリを受信します。

- ・ エラーなし、応答なしセクションを受信しました
 - ・ サーバーが要求を完了できませんでした。応答なしセクション
 - ・ 名前エラー、応答なしセクションを受信しました
 - ・ 機能が実装されていない
 - ・ サーバがクエリへの応答を拒否
-

 注 : AsyncOSは、外部依存関係を評価する前にポリシーに基づいてトランザクションを評価し、アプライアンスからの不要な外部通信を回避します。たとえば、未分類のURLをブロックするポリシーに基づいてトランザクションがブロックされた場合、そのトランザクションはDNSエラーに基づいて失敗することはありません。

プライオリティ:値0が最も高いプライオリティです。両方のプライオリティが同じ場合は、ランダムIPが選択されます。

CLIからのDNSの設定

CLIからdnsconfigを使用して、DNS設定を行うことができます。

手順 1 : CLIで「dnsconfig」と入力します。

```
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.

```
[ ]>
```

ステップ 2 : 新しいDNSサーバーを一覧に追加するには、「NEW」と入力してEnterキーを押します。

ステップ 3 : 新しいネームサーバを追加するプライマリDNSネームサーバまたはセカンダリDNSネームサーバのいずれかを選択します。

```
[ ]> 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
```

ステップ 4 : 新しいネームサーバまたは代替ドメインサーバ (条件付き転送ドメイン名) の追加を選択します。

```
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
```

ステップ 5 : 新しいネームサーバのIPアドレスを入力します。

手順 6 : 新しく追加したネームサーバのプライオリティを入力します。

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

手順 7 : Enterキーを押してウィザードを終了します。

ステップ 8 : commitと入力して、変更を保存します。

注：ネームサーバを編集または削除するには、dnsconfigでEDITとDELETEを選択します。

SETUPオプションでは、DNSキャッシュ時間とオフラインDNS検出設定を次のように設定できます。

```
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]>

DNSキャッシュの最小TTL (秒):このオプションは、SWAがレコードをキャッシュした最小秒数を設定します。詳細については、このドキュメントの「DNSキャッシュ」の項を参照してください。

ローカルDNSサーバーをオフラインと見なす前に失敗した試行回数を入力します。DNSサーバーがDNSクエリに回答しない場合は、カウンタが起動します。

この定義済みの値に達すると、そのネームサーバはオフラインDNSサーバと見なされ、SWAは事前に定義された期間 (次のオプション) の間、そのネームサーバにDNSクエリを送信しなくなります。

DNSサーバがosオフラインとマークされると、次のエラーメッセージが表示されます。

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

オフラインのローカルDNSサーバをポーリングする間隔を秒数で入力します。オフラインとマークされたDNSサーバがこの時間 (秒数) を過ぎると、SWAはそのネームサーバにDNSクエリを送信し始め、DNSサーバの応答失敗カウンタはゼロにリセットされます。

CLI DNSコマンド

手動レコードの作成

手動の「Aレコード」を作成するには、Hostsファイルを使用または編集できません。dnsconfigのlocalhosts隠しコマンドはCLIで使用できます。

注：この設定を変更した後は、変更をコミットする必要があります。

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は、キャッシュされているすべてのDNSレコードをDNSキャッシュテーブルから削除します。

```
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]>

HTTP 307 (Temporary Redirect)ステータスコードは、ターゲットリソースが一時的に異なる Uniform Resource Identifier (URI)の下に存在し、ユーザエージェントがそのURIへの自動リダイレクトを実行する場合は要求メソッドを変更してはならないことを示します。リダイレクトは時間の経過とともに変化する可能性があるため、クライアントは引き続き元の有効な要求URIを使用する必要があります。

詳細：[HTTP 307一時リダイレクトステータスコードとは - Kinsta](#)

これらのオプションは、トランスペアレントプロキシ導入でクライアント要求を評価する際に、SWAが接続先のIPアドレスをどのように決定するかを制御します。要求が受信されると、WSAは宛先IPアドレスとホスト名を確認します。SWAは、TCP接続の元の宛先IPアドレスを信頼するか、独自のDNS解決を実行して解決されたアドレスを使用するかを決定する必要があります。デフォルトは、「0 =常に順番にDNS応答を使用する」です。これは、SWAがクライアントにIPアドレスを提供することを信頼しないことを意味します。

オプション1:SWAはクライアントが指定したIPアドレスで接続を試行しますが、失敗した場合は解決済みのアドレスにフォールバックします。解決されたアドレスは、ポリシー評価(Webカテゴリ、Webレピュテーションなど)に使用されます。

オプション2:SWAは接続にクライアント指定のアドレスのみを使用し、フォールバックしません。解決されたアドレスは、ポリシー評価(Webカテゴリ、Webレピュテーションなど)に使用されます。

オプション3:SWAは接続にクライアント指定のアドレスのみを使用し、フォールバックしません。クライアントが指定したIPアドレスは、ポリシー評価(Webカテゴリ、Webレピュテーションなど)に使用されます。

選択するオプションは、特定のホスト名の解決済みアドレスを決定する際に管理者がクライアントに設定する必要がある信頼度によって異なります。クライアントがダウンストリームプロキシの場合は、不要なDNSルックアップの追加の遅延を回避するためにオプション3を選択します。

DNS キャッシュ

効率性とパフォーマンスを向上させるため、Cisco SWAは最近接続したドメインのDNSエントリを保存します。DNSキャッシュにより、SWAは同じドメインの過度のDNSルックアップを回避で

きます。DNSキャッシュエントリは、レコードのTTL（存続可能時間）が原因で期限切れになります。

DNSサーバのレコードのTTLがSWA dnsconfigキャッシュのTTL時間より大きい場合、DNSキャッシュはDNSサーバからのTTLを使用します。

DNSサーバのレコードのTTLがSWA dnsconfigキャッシュのTTL時間よりも短い場合、DNSキャッシュはWSA dnsconfig設定からのTTLを使用します。

 注意:SWAには2つのDNSキャッシュがあり、1つはプロキシプロセス用に設計されており、もう1つは内部プロセス用に使用されています。

デフォルトでは、SWAはレコードのTTLにかかわらず、最低30分間DNSレコードをキャッシュします。コンテンツ配信ネットワーク(CDN)を多用する最新のWebサイトは、IPアドレスが頻繁に変更されるため、TTLレコードが低くなります。

これにより、クライアントは特定のサーバに対して1つのIPアドレスをキャッシュし、SWAは同じサーバに対して別のアドレスをキャッシュする可能性があります。これに対処するために、dnsconfig CLIコマンドの「SETUP」セクションからSWAのデフォルトTTLを5分に下げることができます。

たとえば、DNS設定の「minimum TTL in seconds for DNS cache」が10分に設定されており、レコードのTTLが5分の場合、キャッシュされたレコードのTTLは10分に増加します。

一方、レコードのTTLが15分に設定されている場合、SWAは15分間のレコードをキャッシュに保存します。

ただし場合によっては、DNS キャッシュでエントリをクリアする必要があります。破損しているかまたは期限切れの DNS キャッシュ エントリが原因で、リモート ホストへの配信で問題が発生することがあります。

通常、この問題が発生するのは、ネットワークの移動またはその他の状況でアプライアンスがオフラインになった後です。

GUIからのDNSキャッシュのクリア

ステップ 1：トップメニューからNetworkを選択します

ステップ 2：DNSを選択します

ステップ 3：Clear DNS Cacheを選択します。

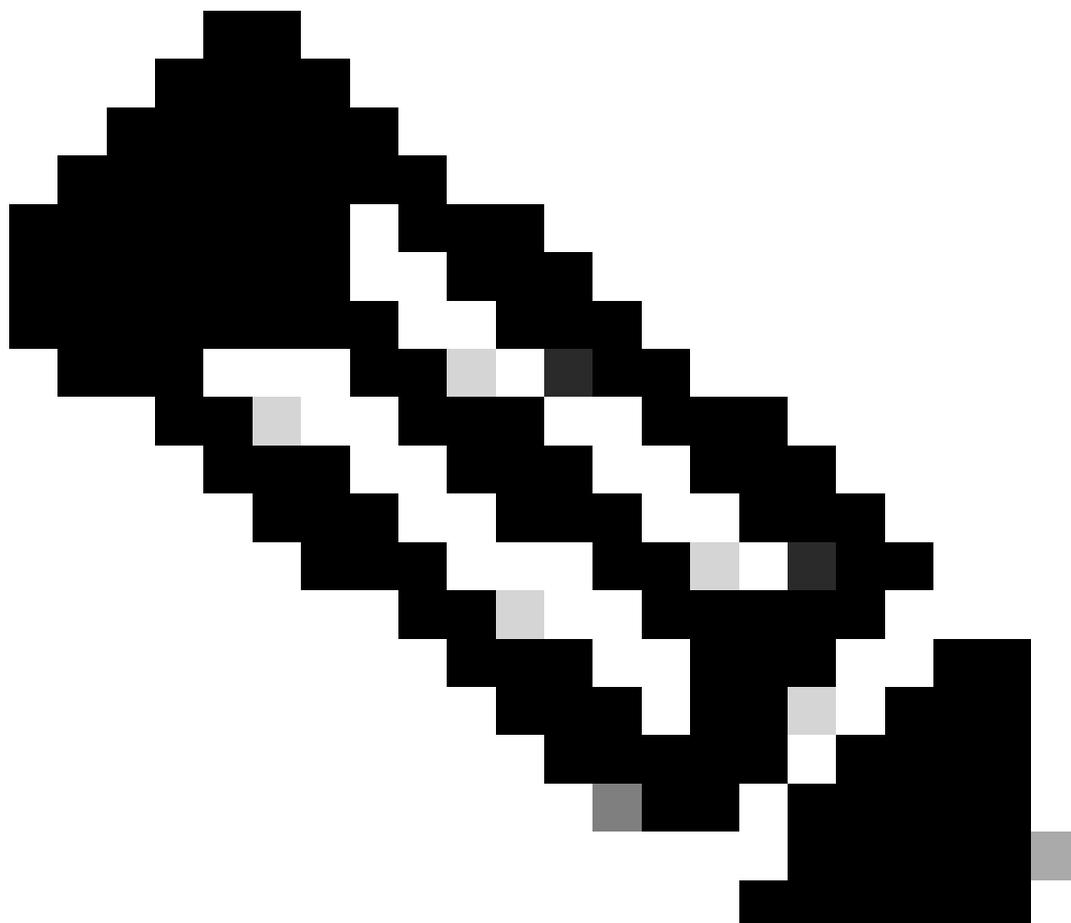
 注意：このコマンドを実行すると、キャッシュの再配置中に一時的にパフォーマンスが低下する場合があります

CLIからのDNSキャッシュのクリア

Cisco WSAのDNSキャッシュをクリアするには、dnsflushcommandをCLIから実行します。

DNSキャッシュの表示

SWAでキャッシュされたDNSレコードをCLIまたはGUIから表示するオプションはありません。



注：nslookupを使用してDNSキャッシュを照会することはできません。

DNSのトラブルシューティング

DNSログの表示

Webプロキシコンポーネントに関連するログの種類の一部が有効になっていません。メイン Webプロキシログタイプ（「デフォルトプロキシログ」と呼ばれる）はデフォルトで有効になっており、すべてのWebプロキシモジュールの基本情報をキャプチャします。

各Webプロキシモジュールには、必要に応じて手動で有効にできる独自のログタイプもあります

。

システムログ、記録DNS、エラー、およびコミットアクティビティ。既定では有効になっていません



ヒント：システムログのログレベルをDEBUGに変更すると、DNSのクエリと応答を確認できます。ログレベルはGUIとCLIから変更できます。

GUIからのシステムログレベルの変更

ステップ 1：トップメニューからSystem Administrationを選択します

ステップ 2：ログサブスクリプションの選択

ステップ 3：System Logsの選択

ステップ 4：Log LevelセクションでDEBUGを選択します

ステップ 5：Submit

手順 6：変更を確定

Edit DNS

DNS Server Settings																			
Primary DNS Servers:	<input checked="" type="radio"/> Use these DNS Servers <table border="1"><thead><tr><th>Priority ?</th><th>Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text" value="0"/></td><td><input type="text" value="10.1.1.1"/></td><td></td></tr><tr><td><input type="text" value="1"/></td><td><input type="text" value="10.2.2.2"/></td><td></td></tr><tr><td><input type="text" value="2"/></td><td><input type="text" value="10.3.3.3"/></td><td></td></tr></tbody></table> <p>Alternate DNS servers Overrides (Optional): Add Row</p> <table border="1"><thead><tr><th>Domain(s)</th><th>DNS Server IP Address(es)</th><th></th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td><td></td></tr></tbody></table> <p><i>i.e., example.com, example2.com</i> <i>i.e., 10.0.0.3 or 2001:420:80:1::5</i></p>	Priority ?	Server IP Address		<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>		<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>		<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>		Domain(s)	DNS Server IP Address(es)		<input type="text"/>	<input type="text"/>	
Priority ?	Server IP Address																		
<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>																		
<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>																		
<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>																		
Domain(s)	DNS Server IP Address(es)																		
<input type="text"/>	<input type="text"/>																		
	<input type="radio"/> Use the Internet's Root DNS Servers <p>Alternate DNS servers Overrides (Optional): Add Row</p> <table border="1"><thead><tr><th>Domain</th><th>DNS Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td><td></td></tr></tbody></table> <p>DNS Server FQDN <input type="text"/></p> <p><i>i.e., dns.example.com</i></p>	Domain	DNS Server IP Address		<input type="text"/>	<input type="text"/>													
Domain	DNS Server IP Address																		
<input type="text"/>	<input type="text"/>																		
Secondary DNS Servers:	<table border="1"><thead><tr><th>Priority ?</th><th>Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text" value="0"/></td><td><input type="text" value="10.10.10.10"/></td><td></td></tr></tbody></table> Add Row	Priority ?	Server IP Address		<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>													
Priority ?	Server IP Address																		
<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>																		
Routing Table for DNS Traffic:	Management																		
IP Address Version Preference:	<input checked="" type="radio"/> Prefer IPv4 <input type="radio"/> Prefer IPv6 <input type="radio"/> Use IPv4 only <p><i>This preference applies when DNS results provide both IPv4 and IPv6 address for host. When selecting Prefer IPv4 or Prefer IPv6, ensure that the appliance network settings are configured appropriately to support IPv6.</i></p>																		
Secure DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <p><i>SECURE DNS protects DNS data. It uses the DNSSEC protocol to strengthen the authentication in the DNS using digital signatures. If DNSSEC is enabled, fallback of DNSSEC query to DNS query will not occur. Supported DNSSEC Algorithms: DSA, DSA_NSEC3, ED448, ED25519, ECDSAP256SHA256, ECDSAP384SHA384, RSASHA1, RSASHA1_NSEC3, RSASHA256, RSASHA512.</i></p>																		
Wait Before Timing out Reverse DNS Lookups:	<input type="text" value="2"/> seconds																		
Domain Search List: ?	<input type="text"/> <p><i>Separate multiple entries with commas. Maximum allowed characters 2048.</i></p>																		

Cancel Submit

イメージ : システムログ、ログレベルの変更

CLIからのシステムログレベルの変更

ステップ 1 : CLIへのログイン

ステップ 2 : logconfigと入力します。

ステップ 3 : EDITを選択します

ステップ 4 : System_Logsに関連付けられている番号を入力します

ステップ 5 : ログレベルになるまでEnterキーを押します

手順 6 : 番号4のデバッグを選択します

手順 7 : ウィザードを終了するまでEnterキーを押します

ステップ 8 : 変更を保存するには、commitと入力します。

```
SWA_CLI> logconfig

Currently configured logs:
...
42. "system_logs" Type: "System Logs" Retrieval: FTP Poll
...

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[ ]> EDIT

Enter the number of the log you wish to edit:
[ ]> 42 <--- in this example the System_logs is number 42

Please enter the name for the log:
[system_logs]>

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
....
SWA_CLI> commit
```

 ヒント : トラブルシューティングを終了したら、ログレベルをInformationに戻してください。戻さないと、ディスクの入出力(I/O)に大きな負荷がかかり、ログファイルが高速に読み込まれます。

nslookup

nslookupコマンドを使用して、異なるFQDNに対するSWAの名前解決の応答を確認します。

この例では、名前を解決する最初の試みでTTLが30分に設定されています。

2回目の試行では、TTLが30分未満であることが確認できます。これは、このレコードがキャッシュから解決されたことを示します。

```
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
```

掘る

digは、DNSレコードを照会するもう1つの便利なコマンドです。digコマンドを使用すると、クエリーを送信する送信元インターフェイスまたはDNSサーバを指定できます。

この例では、サーバ10.1.1.1からのA-Recordに対するクエリを次に示します

```
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
```

digの使用方法 :

```
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

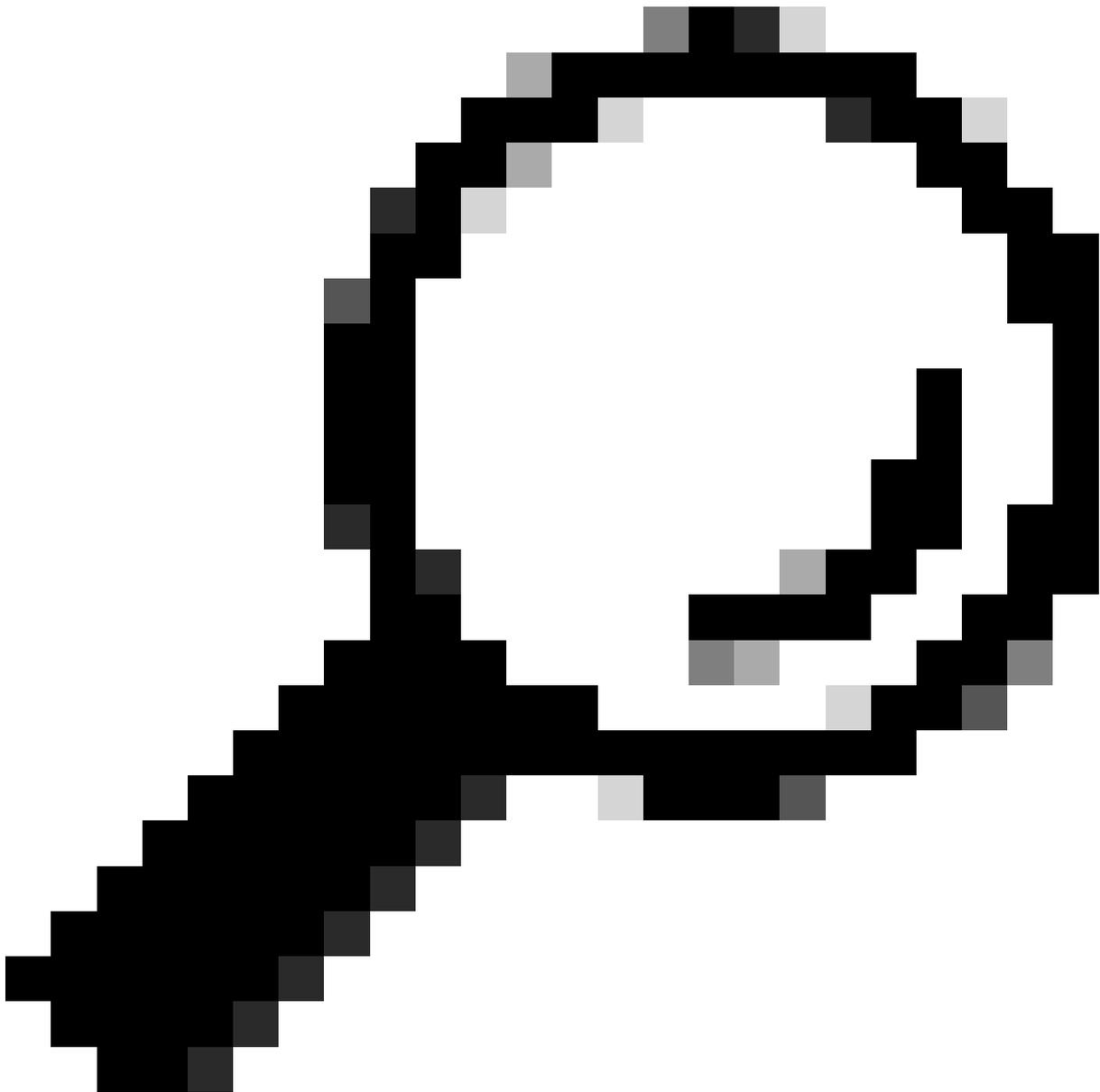
Specify the source IP address.

-t

Make query over tcp.

-x IP Address

Do a reverse lookup on this IP address.



ヒント：発信元IPを選択すると、名前解決を照会するインターフェイスを選択できます。

DNS応答が遅い

すべてのURLまたは一部のURLの読み込みに時間がかかる場合（同じページを更新する場合と比較して）、DNS応答時間を確認することをお勧めします。SWAには、DNS応答時間を確認する次の2つのオプションがあります。

- AccessLogsのカスタムフィールドを構成します。
- Trackstatログ。

DNS統計情報を表示するためのアクセスログの変更

各Web要求のDNS時間を表示するようにアクセスログを変更できます。

ステップ 1 : GUIにログインします。

ステップ 2 : [システム管理]メニューから、[ログサブスクリプション]を選択します。

ステップ3:Log Name列から、accesslogs、または新しく作成したログの名前をクリックします。
この例では、TAC_access_logsです。

ステップ4:カスタムフィールドのセクションで、次の文字列を貼り付けます。

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

ステップ5 : 変更を送信し、確定します。

カスタムフィールド名	カスタムフィールド	W3Cログ	説明
DNS応答	%:<d	x-p2p-dns-wait-time	Webプロキシがドメイン名要求(DNS)要求をWebプロキシDNSプロセスに送信するのにかかった時間。
DNS合計	%:>d	x-p2p-dns-svc-time	WebプロキシDNSプロセスがDNSの結果をWebプロキシに返信するのにかかった時間。

アクセスログのカスタムフィールドを編集する方法の詳細については、次のリンクを参照してください。[アクセスログのパフォーマンスパラメータの設定 - シスコ](#)

TrackstatログのDNS応答時間の概要

DNSサービスおよびその他の内部サービスの統計情報は、trackstatログで表示できます。SWAにFTPで接続すると、trackstatsログにアクセスできます。

この例では、SWAが最後にリポートされてからのDNSサーバからの経過時間によって分類された、キャッシュの統計情報とDNS応答の数を確認できます。

```
...  
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
```

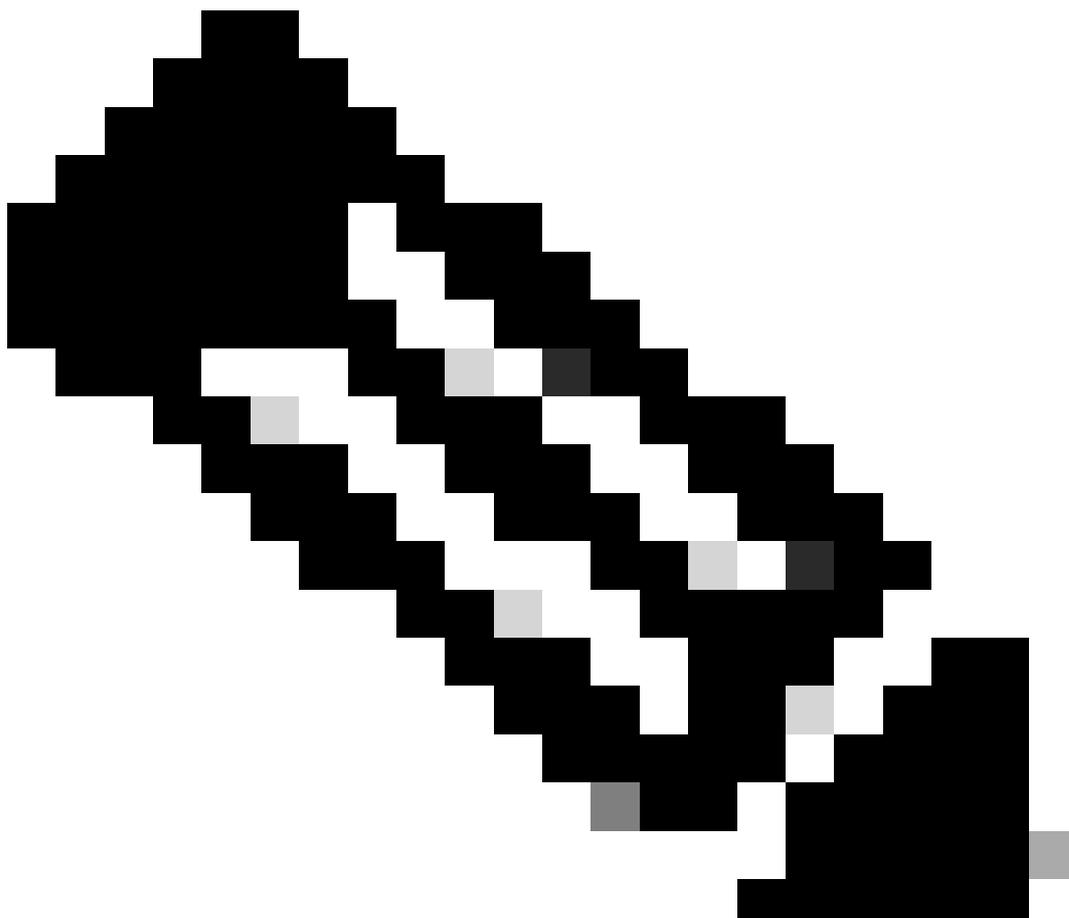
DNS Time	4.0 ms	32
DNS Time	6.3 ms	35
DNS Time	10.0 ms	37
DNS Time	15.8 ms	301
DNS Time	25.1 ms	80
DNS Time	39.8 ms	136
DNS Time	63.1 ms	91
DNS Time	100.0 ms	12
DNS Time	158.5 ms	33
DNS Time	251.2 ms	14
DNS Time	398.1 ms	12
DNS Time	631.0 ms	45
DNS Time	1000.0 ms	120
DNS Time	1584.9 ms	73
DNS Time	2511.9 ms	296
DNS Time	3981.1 ms	265
DNS Time	6309.6 ms	190

たとえば、最後の行では、SWAが最後にリポートされてから190のDNSクエリが6,309ミリ秒 (約6秒) 以上完了したことを示しています。

期間内の正確な数値を求めるには、開始時間と終了時間の値を減算します。

たとえば、DNS応答時間を10:00 AMから11:00 AMの間で特定するには、11:00 AMの統計情報を収集して、10:00 AMの統計情報から差し引きます。

その結果、目的の日付の午前10:00から午前11:00までのDNS応答時間が得られます。



注：追跡統計情報ログは5分ごとに収集されます。

パケット キャプチャ

パケットをキャプチャしてDNSの要求と応答を表示し、使用できるDNSのみのフィルタリングを行うことができます(ポート53)。

GUIからパケットキャプチャを開始するには、次の手順を実行します。

ステップ 1：右上からサポートとヘルプを選択します。

ステップ 2：パケットキャプチャの選択

ステップ3: (オプション) Edit Settingsを選択してフィルタを追加します

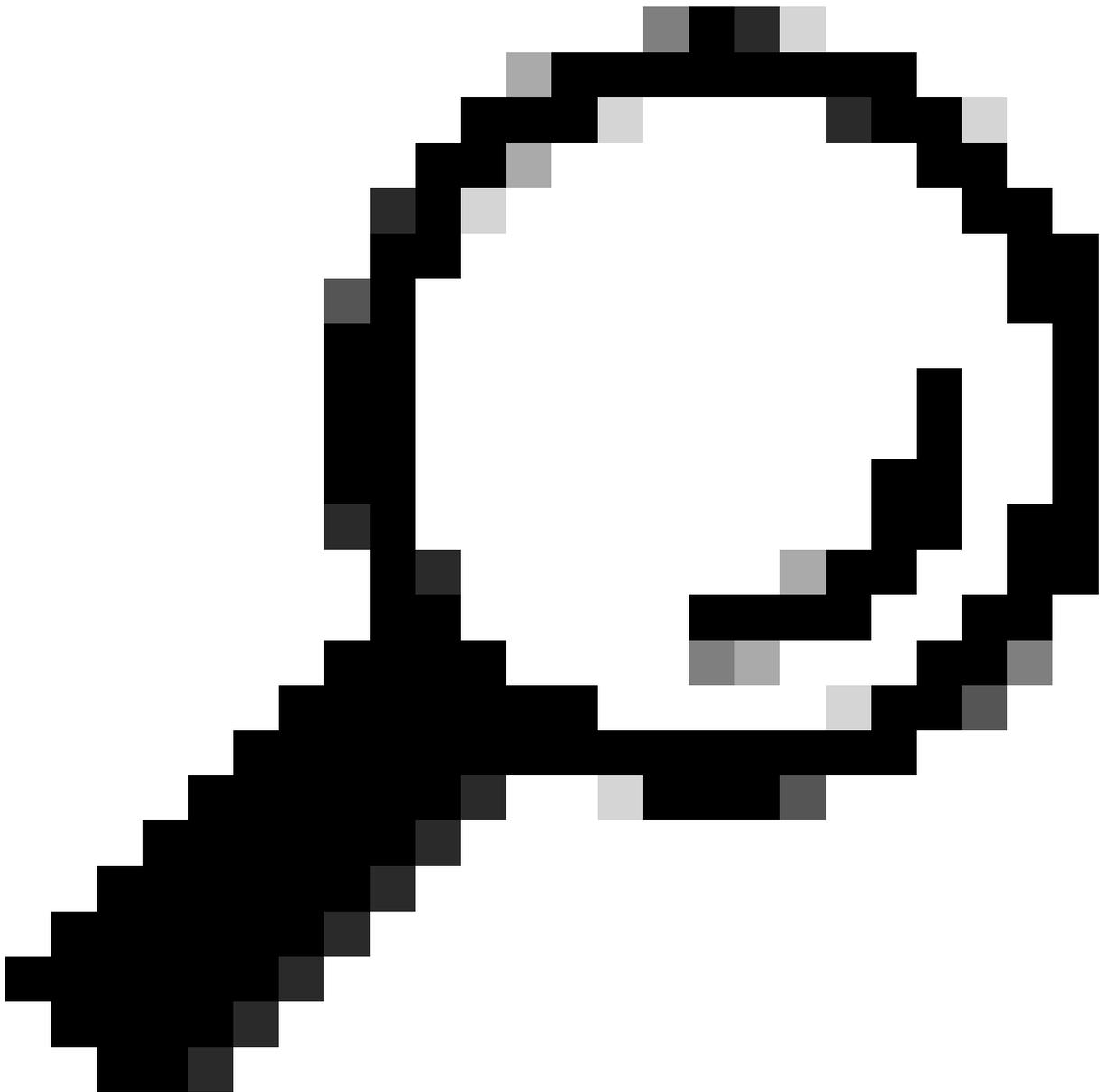
ステップ4: (オプション) インターフェイスを選択し、カスタムフィルタセクションにport 53と入力します

ステップ5: (オプション) 「送信」を選択します

Edit Packet Capture Settings

Packet Capture Settings	
Capture File Size Limit: ?	<input type="text" value="200"/> MB <small>Maximum file size is 200MB</small>
Capture Duration:	<input type="radio"/> Run Capture Until File Size Limit Reached <input type="radio"/> Run Capture Until Time Elapsed Reaches <input type="text"/> (e.g. 120s, 5m 30s, 4h) <input checked="" type="radio"/> Run Capture Indefinitely <small>The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.</small>
Interfaces:	<input checked="" type="checkbox"/> M1 <input type="checkbox"/> P1 <input type="checkbox"/> P2
Packet Capture Filters	
Filters:	<small>All filters are optional. Fields are not mandatory.</small> <input type="radio"/> No Filters <input type="radio"/> Predefined Filters ? Ports: <input type="text"/> Client IP: <input type="text"/> Server IP: <input type="text"/> <input checked="" type="radio"/> Custom Filter ? <input type="text" value="port 53"/>
<small>Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.</small>	
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

イメージ : DNSパケットをキャプチャするフィルタの追加



ヒント：パケットキャプチャの設定は、送信後すぐに使用できます。変更をコミットして、今後も使用できるように設定を永続的に保存します。

手順 6：Start Captureを選択します。

ステップ7: (オプション) 特定のサイトまたはURLアクセスのトラブルシューティングが必要な場合は、トラフィックを生成します。

ステップ 8：キャプチャの停止

ステップ 9：ページが更新されるのを待ってから、「Manage Packet Capture Files」リストから最初のパケットキャプチャを選択します

ステップ 10：Download Fileを選択します。

L4TM

レイヤ4トラフィックモニタは、各セキュアWebアプライアンスのすべてのポートから受信するネットワークトラフィックをリッスンし、ドメイン名とIPアドレスを自身のデータベーステーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

内部クライアントがマルウェアに感染し、標準外のポートやプロトコルを介してオートコールを試みると、L4トラフィックモニタによって、企業ネットワークから出るためのオートコールが阻止されます。

デフォルトでは、L4トラフィックモニタが有効になっており、DNSやその他のサービスを含むすべてのポートでトラフィックをモニタするように設定されています。

レイヤ4トラフィックモニタの詳細については、ユーザガイドを参照してください。

Errors

通知ページ

デフォルトでは、SWAは通知ページを表示して、ユーザにブロックされたことを通知し、ブロックの理由を通知します

ファイル名と通知タイトル:ERR_DNS_FAIL (DNSエラー)

説明 : 要求されたURLに無効なドメイン名が含まれている場合に表示されるエラーページ。

通知テキスト : このホスト名<hostname >のホスト名解決 (DNSルックアップ) が失敗しました。

インターネットアドレスのスペルが間違っているか古いか、ホスト<hostname >が一時的に使用できないか、DNSサーバが応答しない可能性があります。

入力したインターネットアドレスのスペルを確認してください。正しい場合は、後でこの要求を試してください。

This Page Cannot Be Displayed

The host name resolution (DNS lookup) for this host name (invalidurl.cisco.com) has failed. The Internet address may be misspelled or obsolete, the host (invalidurl.cisco.com) may be temporarily unavailable, or the DNS server may be unresponsive.

Please check the spelling of the Internet address entered. If it is correct, try this request later.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Sun, 02 Jul 2023 12:16:14 CEST

Username:

Source IP: 10.61.66.65

URL: GET http://invalidurl.cisco.com/

Category: Computers and Internet

Reason: UNKNOWN

Notification: DNS_FAIL

☒ - DNS FAILエラー

アクセスログの結果コードなし

アクセスログファイル内のトランザクション結果コードは、アプライアンスがクライアント要求を解決する方法を説明します。アクセスログ内の結果コードがNONEの場合、これはトランザクションにエラーがあったことを意味します。たとえば、DNS障害やゲートウェイのタイムアウトが発生した場合です。

```
1688292974.527 20 10.61.66.65 NONE/503 0 GET http://invalidurl.cisco.com/ - NONE/invalidurl.cisco.com -
```

DNSキャッシュをブートストラップできませんでした

アプライアンスのリポート時に「Failed to bootstrap the DNS cache」というメッセージが表示されるアラートが生成された場合は、システムがプライマリDNSサーバに接続できなかったことを意味しています。

これは、ネットワーク接続が確立される前にDNSサブシステムがオンラインになった場合に、ブート時に発生する可能性があります。このメッセージがそれ以外の場合は、ネットワークに問題があるか、またはDNS設定が有効なサーバに設定されていないことを示しています

DNSサーバーのクエリの最大失敗数に達しました

SWAで設定された1台または複数のDNSサーバがDNSクエリに応答しなかった場合、SWAはそれ

らのサーバをオフラインと見なし、事前に定義された時間はDNSクエリを送信しません。詳細については、この記事の「CLIからのDNSの設定」を参照してください。

DNS_FAIL

SWAがHTTP要求を受信し、ホスト名の解決に失敗すると、デフォルトではSWAは次のような応答を返します。

```
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
```

この機能は「サーバ名拡張」と呼ばれます。

WSAは、リダイレクトされたホスト名がクライアントの予期されるページを解決する試みでこれを実行します。

「DNSルックアップが失敗した場合のHTTP 307リダイレクションのURL形式」を変更して、詳細を確認できます。この記事の「advanceproxyconfig」セクションを参照してください。

WSAは、ServFailを返すDNS要求を障害として扱います。

たとえば、NXDOMAINは「SERVER_NAME_EXPANSION」ではなく「DNS_FAIL」を返します。

関連情報

[AsyncOS 15.0 for Cisco Secure Web Appliance ユーザガイド](#)

[セキュアなWebアプライアンスのベストプラクティスの使用：シスコ](#)

[Cisco Content Hub – ドメインネームシステムの概要](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。