

# ASA での DNS Doctoring の設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[DNS Doctoring の例](#)

[ASA 内部の DNS サーバ](#)

[ASA 外部の DNS サーバ](#)

[VPN NAT および DNS Doctoring](#)

[関連情報](#)

## 概要

このドキュメントでは、ドメイン ネーム システム ( DNS ) 応答に埋め込まれている IP アドレスを変更するために、適応型セキュリティ アプライアンス ( ASA ) で DNS Doctoring を使用し、クライアントがサーバの正しい IP アドレスに接続できるようにする方法について説明します。

## 前提条件

### 要件

DNS Doctoring では、DNS インспекションを有効にするだけでなく、ASA で Network Address Translation ( NAT ) を設定する必要があります。

### 使用するコンポーネント

このドキュメントの情報は、適応型セキュリティ アプライアンスに基づくものです。

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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### 表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## DNS Doctoring の例

## [ASA 内部の DNS サーバ](#)

```
図 1 nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

図 1 の DNS サーバはローカル管理者によって制御されています。DNS サーバはプライベート IP アドレスを配布する必要があります。これは、アプリケーション サーバに割り当てられる実際の IP アドレスです。これにより、ローカル クライアントはアプリケーション サーバに直接接続することができます。

ただし、リモート クライアントはプライベート アドレスを使用してアプリケーション サーバにアクセスすることはできません。そのため、DNS の応答パケットに埋め込まれている IP アドレスを変更するために、ASA 上に DNS Doctoring を設定します。これにより、リモート クライアントが `www.abc.com` に対して DNS 要求を行った場合、取得する応答は、アプリケーション サーバの変換されたアドレスになります。NAT ステートメントで DNS キーワードを指定しない場合、リモート クライアントは `10.1.1.100` に接続しようとしませんが、このアドレスはインターネット上ではルートできないため、接続はできません。

## [ASA 外部の DNS サーバ](#)

```
図 2 nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

図 2 の DNS サーバは ISP または類似のサービス プロバイダーによって制御されています。DNS サーバはパブリック IP アドレス、つまりアプリケーション サーバの変換された IP アドレスを配布する必要があります。これにより、すべてのインターネット ユーザがインターネットを介してアプリケーション サーバにアクセスできるようになります。

ただし、ローカル クライアントはパブリック アドレスを使用してアプリケーション サーバにアクセスすることはできません。そのため、DNS の応答パケットに埋め込まれている IP アドレスを変更するために、ASA 上に DNS Doctoring を設定します。これにより、ローカル クライアントが `www.abc.com` に対して DNS 要求を行った場合、受信する応答は、アプリケーション サーバの実際のアドレスになります。NAT ステートメントで DNS キーワードを指定しない場合、ローカル クライアントは `198.51.100.100` に接続しようとし、ただし、このパケットは ASA へ送信されるため接続が失敗し、パケットがドロップします。

## [VPN NAT および DNS Doctoring](#)

図3  
重複しているネットワークがある状況を考えてみます。ここでは、リモート側とローカル側の両方にアドレス `10.1.1.100` があります。そのため、ローカル サーバ上で NAT を実行し、リモート クライアントが IP アドレス `192.1.1.100` に継続してアクセスできるようにする必要があります。これが正しく作動するためには、DNS Doctoring が必要です。

この機能では、DNS Doctoring は実行できません。DNS キーワードは、オブジェクト NAT またはソース NAT の最後にのみ追加できます。Twice NAT は DNS キーワードをサポートしていません。可能な設定が 2 つありますが、両方とも失敗します。

失敗した設定 1：最後の行を設定すると、リモート クライアントに対してだけでなく、インター

ネット上のすべてのクライアントに対して 10.1.1.1 が 192.1.1.1 に変換されます。192.1.1.1 はインターネットでルートできないため、インターネット上のどのクライアントもローカルサーバにアクセスできません。

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
    REMOTE_CLIENT REMOTE_CLIENT
```

**失敗した設定 2：** 必要な Twice NAT 行の後に DNS Doctoring の NAT 行を設定すると、DNS Doctoring が絶対に作動しない状況になります。結果として、リモートクライアントは IP アドレス 10.1.1.100 で www.abc.com にアクセスしようとしませんが、これは機能しません。

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
    REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

## **関連情報**

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス > ソフトウェア ダウンロード](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)