

# PIX/ASA : static コマンドおよび 2 つの NAT インターフェイスによる DNS Doctoring の設定例

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[背景説明](#)

[シナリオ: 2 NAT insideoutside](#)

[トポロジ](#)

[問題 : クライアントが WWW サーバにアクセスできない](#)

[ソリューション : 「dns」 キーワード](#)

[別のソリューション : ヘアピニング](#)

[DNS インспекションの設定](#)

[スプリット DNS の設定](#)

[確認](#)

[DNS トラフィックのキャプチャ](#)

[トラブルシューティング](#)

[DNS 書き換えが実行されない](#)

[変換の作成に失敗する](#)

[ドロップする UDP DNS 応答](#)

[関連情報](#)

## [はじめに](#)

このドキュメントでは、ASA 5500 シリーズ適応型セキュリティ アプライアンスまたは PIX 500 シリーズ セキュリティ アプライアンスで、スタティック ネットワーク アドレス変換 ( NAT ) ステートメントを使用してドメイン ネーム システム ( DNS ) Doctoring を実行するための設定例について説明します。DNS Doctoring により、セキュリティ アプライアンスは DNS A レコードを書き換えられます。

DNS 書き換えでは、次の 2 つの機能が実行されます。

- DNS クライアントがプライベート インターフェイス上に存在する場合、DNS 応答に含まれるパブリック アドレス ( ルーティング可能なアドレスまたはマップ アドレス ) をプライベート アドレス ( リアル アドレス ) に変換する。
- DNS クライアントがパブリック インターフェイス上に存在する場合、プライベート アドレスをパブリック アドレスに変換する。

注: この資料の設定は 2 つの NAT インターフェイスが含まれています; 中および外部で。静的アドレスおよび 3 つの NAT インターフェイスと治療する DNS の例に関しては ( 中、外部および dmz )、[PIX/ASA を参照して下さい: 治療する static コマンドおよび 3 つの NAT インターフェイス設定例と DNS を行って下さい。](#)

セキュリティ アプライアンスで NAT を使用する方法についての詳細は、『[PIX/ASA 7.x の NAT と PAT の設定例](#)』および『[PIX での nat、global、static、conduit、および access-list の各コマンドとポートリダイレクション \( フォワーディング \) の使用方法](#)』を参照してください。

## 前提条件

### 要件

セキュリティ アプライアンスで DNS Doctoring を実行するには、DNS インスペクションをイネーブルにする必要があります。デフォルトでは、DNS インスペクションはオンになっています。DNS インスペクションがオフになっている場合は、このドキュメントの「[DNS インスペクションの設定](#)」セクションを参照してください。DNS インスペクションがイネーブルになっている場合、セキュリティ アプライアンスでは次のタスクが実行されます。

- **static** および **nat** コマンドを使用して作成された設定に基づいて DNS レコードを変換します ( DNS 書き換え )。変換は DNS 応答の A レコードだけに適用されます。そのため、PTR レコードを要求する逆参照は DNS 書き換えの影響を受けません。注: 各 A レコードには複数の PAT ルールが適用可能であり、使用する PAT ルールがあいまいになるため、DNS 書き換えはスタティック Port Address Translation ( PAT; ポート アドレス変換 ) と互換性がありません。
- DNS メッセージの最大長を適用します ( デフォルトは 512 バイト、最大長は 65535 バイトです )。設定された最大長よりもパケットの長さが短いことを確認するために、必要に応じて再構成が実行されます。最大長を超えるパケットは廃棄されます。注: 最大長オプションを指定せずに **If you issue the inspect dns** コマンドを発行した場合、DNS パケットのサイズはチェックされません。
- ドメイン名の長さを 255 バイトに、ラベルの長さを 63 バイトに制限します。
- DNS メッセージで圧縮ポインタが見つかった場合、ポインタによって参照されているドメイン名の整合性を確認します。
- 圧縮ポインタのループが存在するかどうかを確認します。

### 使用するコンポーネント

このドキュメントの情報は ASA 5500 シリーズ セキュリティ アプライアンス バージョン 7.2(1) に基づくものです。

本書の情報は、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、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

### 関連製品

この設定は、Cisco PIX 500 シリーズ セキュリティ アプライアンス バージョン 6.2 以降にも適用できます。

注: Cisco Adaptive Security Device Manager(ASDM; Cisco Adaptive Security デバイス マネージャ) の設定はバージョン 7.x だけに適用できます。

## 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。

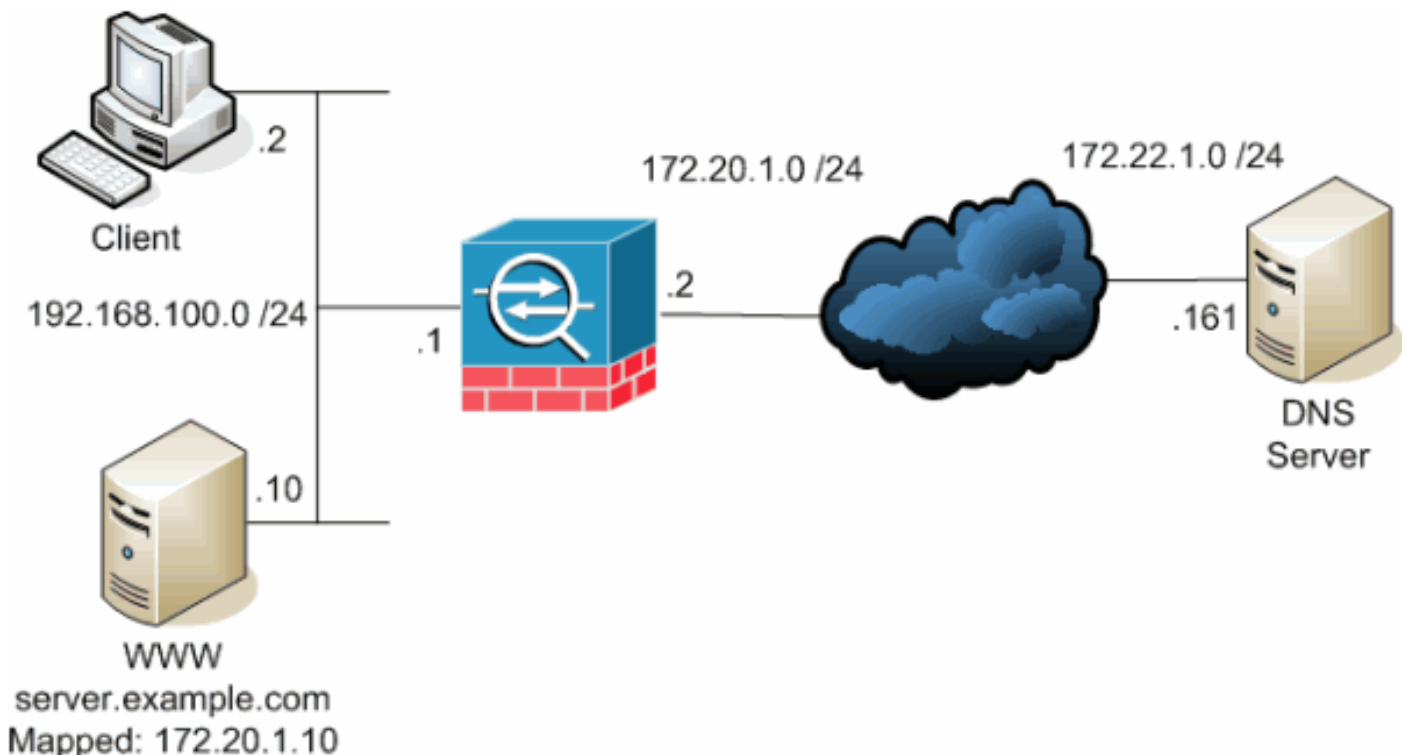
## 背景説明

一般的な DNS 交換においては、クライアントが DNS サーバーに URL またはホスト名を送信し、そのホストの IP アドレスを調べます。DNS サーバは要求を受信し、そのホストの名前と IP アドレスのマッピングを参照して、IP アドレスを含む A レコードをクライアントに提供します。この手順はほとんどの状況において問題なく実行されますが、場合によっては問題が発生することもあります。クライアントと、そのクライアントがアクセスしようとしているホストの両方が NAT の背後にある同一のプライベート ネットワーク上に存在し、クライアントによって使用される DNS サーバが他のパブリック ネットワーク上に存在する場合は、そのような問題が発生します。

## シナリオ: 2 つの NAT インターフェイス ( inside、outside )

### トポロジ

このシナリオでは、クライアントと、クライアントがアクセスしようとしている WWW サーバは、どちらも ASA の inside インターフェイス上に存在しています。クライアントがインターネットにアクセスできるようにダイナミック PAT が設定されています。サーバがインターネットにアクセスできるように (さらに、インターネット ホストが WWW サーバにアクセスできるように)、アクセスリストを含むスタティック NAT が設定されています。



この図は、この状況の例です。この場合、192.168.100.2 のクライアントが `server.example.com` という URL を使用して 192.168.100.10 の WWW サーバにアクセスしようとしています。クラ

クライアントの DNS サービスは、172.22.1.161 の外部 DNS サーバによって提供されます。この DNS サーバは他のパブリック ネットワーク上に存在するため、WWW サーバのプライベート IP アドレスを認識していません。ただし、WWW サーバのマップ アドレス ( 172.20.1.10 ) は認識しています。そのため、この DNS サーバには `server.example.com` を 172.20.1.10 に変換する IP アドレスと名前のマッピングが含まれています。

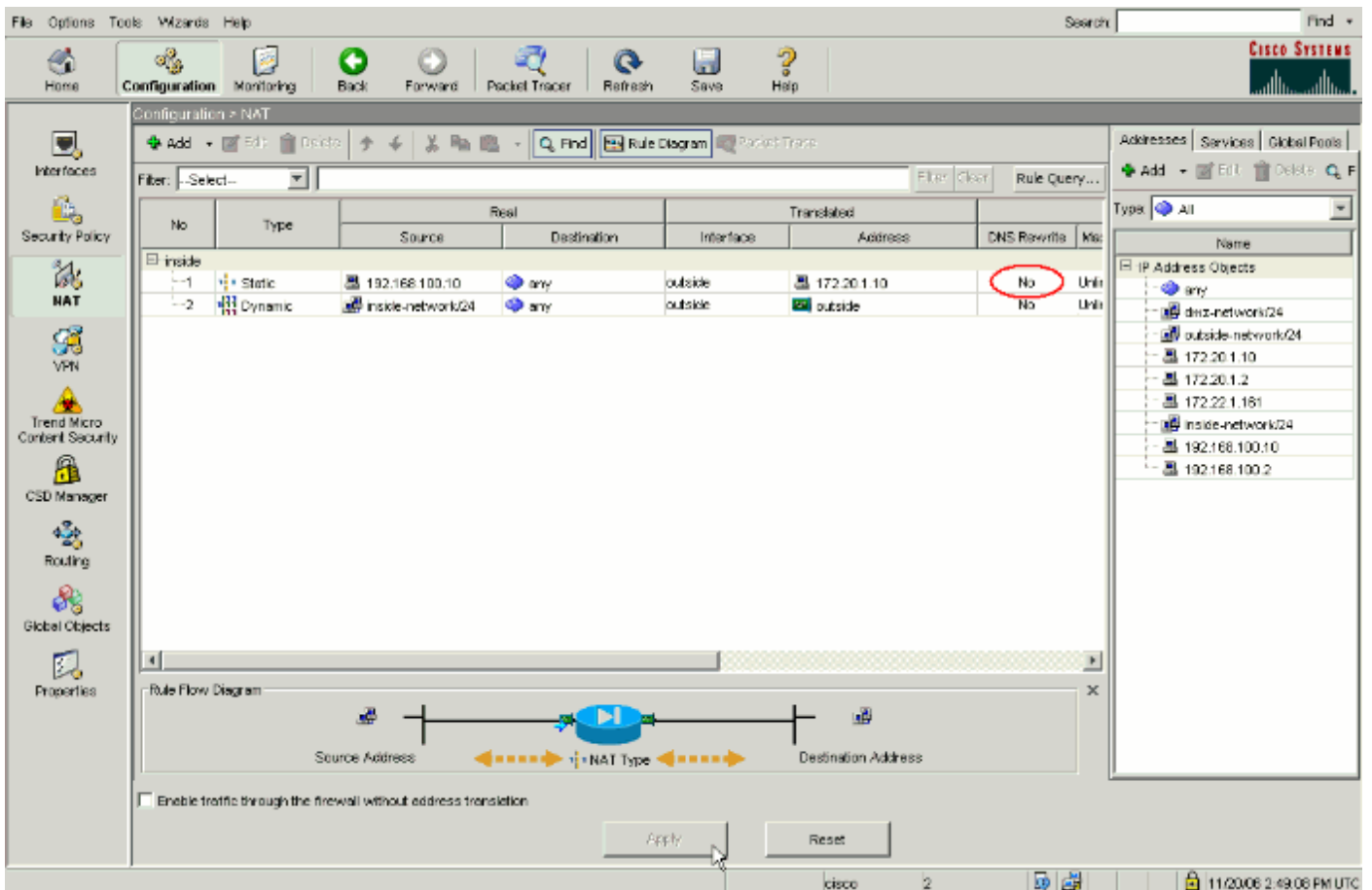
## 問題：クライアントが WWW サーバにアクセスできない

この状況で DNS Doctoring やその他のソリューションが無効になっていない場合、クライアントから `server.example.com` の IP アドレスに関する DNS 要求が送信されても、クライアントは WWW サーバにアクセスできません。これはクライアントがマッピングされたパブリックアドレスが含まれているレコードを受け取るという理由によります: WWW サーバの 172.20.1.10。クライアントがこの IP アドレスにアクセスしようとする、同じインターフェイスでのパケットリダイレクションが許可されないため、セキュリティ アプライアンスによってパケットが廃棄されます。DNS Doctoring がイネーブルになっていない場合、設定の NAT 部分は次のようになります。

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
```

```
!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 access-group OUTSIDE
in interface outside !--- Output suppressed.
```

DNS Doctoring がイネーブルになっていない場合、ASDM の設定は次のようになります。



DNS Doctoring がイネーブルになっていない場合、イベントの packets キャプチャは次のようになります。

### 1. クライアントが DNS クエリーを送信します。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.100.2	172.22.1.161	DNS	Standard query A server.example.com

```

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53)
Domain Name System (query)

```

```

[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

```

```

Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)

```

2. DNS クエリーに対する PAT が ASA によって実行され、クエリーが転送されます。パケットの送信元アドレスが ASA の outside インターフェイスに変更されていることに注意してください。

No.	Time	Source	Destination	Protocol	Info
-----	------	--------	-------------	----------	------



```
Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879)
Domain Name System (response)
  [Request In: 1]
  [Time: 0.005264000 seconds]
  Transaction ID: 0x0004
  Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    server.example.com: type A, class IN
      Name: server.example.com
      Type: A (Host address)
      Class: IN (0x0001)
Answers
    server.example.com: type A, class IN, addr 172.20.1.10
      Name: server.example.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 1 hour
      Data length: 4
      Addr: 172.20.1.10
```

5. この時点で、クライアントは 172.20.1.10 の WWW サーバにアクセスしようとしています。ASA がこの通信の接続エントリを作成します。ただし、inside から outside を経由して inside にトラフィックを流すことは許可されないため、接続はタイムアウトします。ASA ログには次のように表示されます。

```
%ASA-6-302013: Built outbound TCP connection 54175 for
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)
```

```
%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80 to
inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

## ソリューション: 「dns」キーワード

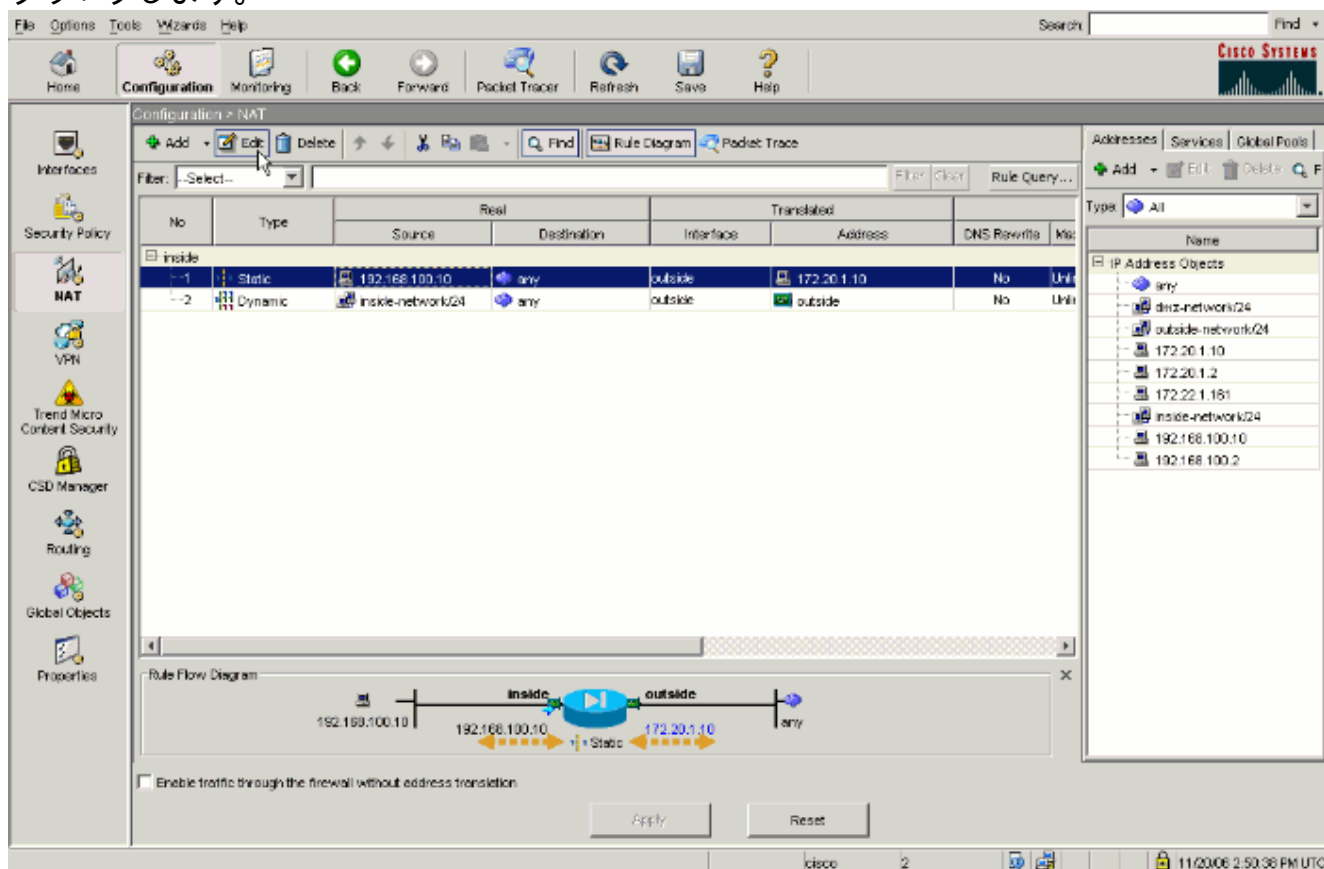
### 「dns」キーワードを使用した DNS Doctoring

dns キーワードを伴う DNS Doctoring では、セキュリティ アプライアンスが DNS サーバからクライアントへの応答を代行受信して、内容を書き換えられるようになります。正しく設定されたとき、セキュリティ アプライアンスは [問題](#) に記述されているようにクライアントをそのような場合には可能にするためにレコードを変更することができます: [クライアントは接続するために WWW サーバセクションにアクセスできません](#)。この状況で DNS Doctoring がイネーブルになっている場合、セキュリティ アプライアンスは、172.20.1.10 ではなく 192.168.100.10 にクライアントを誘導するように A レコードを書き換えます。DNS Doctoring は、スタティック NAT 設定に dns キーワードを追加するとイネーブルになります。DNS Doctoring がイネーブルになっている場合、設定の NAT 部分は次のようになります。

```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
```

*!--- Output suppressed.* access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www *!--- Output suppressed.* global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0 static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 **dns**  
*!--- The "dns" keyword is added to instruct the security appliance to modify !--- DNS records related to this entry.* access-group OUTSIDE in interface outside *!--- Output suppressed.*  
ASDM で DNS Doctoring を設定するには、次の手順を実行します。

1. Configuration > NAT に移動し、修正するスタティック NAT ルールを選択します。[Edit] をクリックします。



2. NAT Options..... をクリックします。



**Edit Static NAT Rule**

Real Address

Interface: inside

IP Address: 192.168.100.10

Netmask: 255.255.255.255

Static Translation

Interface: outside

IP Address: 172.20.1.10

Enable Port Address Translation (PAT)

Protocol: TCP tcp

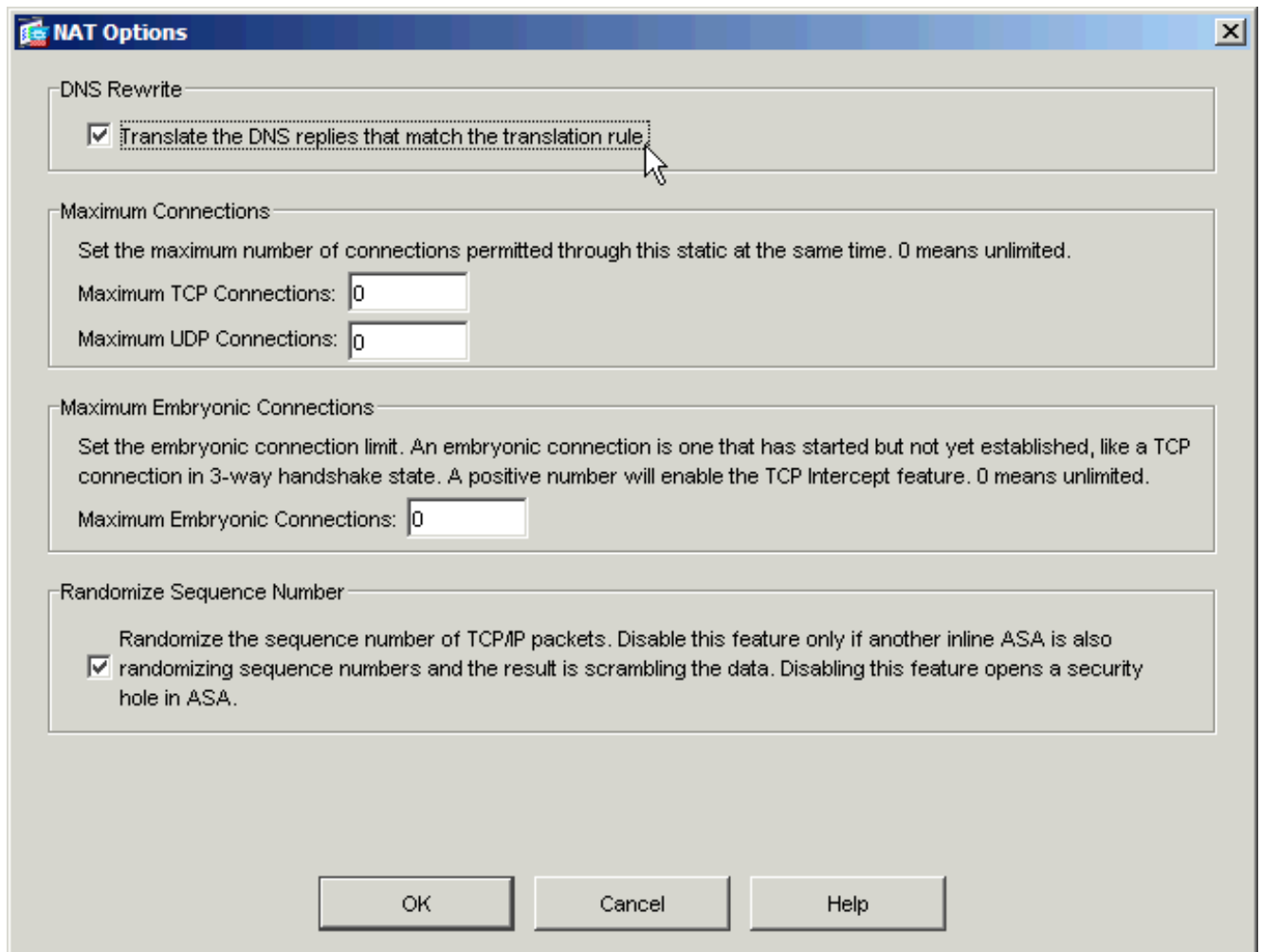
Original Port:

Translated Port:

NAT Options...

OK Cancel Help

3. Translate DNS replies that match the rule チェックボックスにチェックマークを付けます。



4. **OK** をクリックして、NAT Options ウィンドウを閉じます。 **OK** をクリックして、Edit Static NAT Rule ウィンドウを閉じます。 **Apply** をクリックして、セキュリティ アプライアンスに設定を送信します。

DNS Doctoring がイネーブルになっている場合、イベントのパケット キャプチャは次のようになります。

1. クライアントが DNS クエリーを送信します。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.100.2	172.22.1.161	DNS	Standard query A server.example.com

```

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53)
Domain Name System (query)
  [Response In: 2]
  Transaction ID: 0x000c
  Flags: 0x0100 (Standard query)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
Queries
  server.example.com: type A, class IN
    Name: server.example.com
    Type: A (Host address)
    Class: IN (0x0001)

```

2. DNS クエリーに対する PAT が ASA によって実行され、クエリーが転送されます。パケットの送信元アドレスが ASA の outside インターフェイスに変更されていることに注意してください。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	<b>172.20.1.2</b>	172.22.1.161	DNS	Standard query A server.example.com

```
Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22 (00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161 (172.22.1.161)
User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53)
Domain Name System (query)
  [Response In: 2]
  Transaction ID: 0x000c
  Flags: 0x0100 (Standard query)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    server.example.com: type A, class IN
      Name: server.example.com
      Type: A (Host address)
      Class: IN (0x0001)
```

3. DNS サーバが WWW サーバのマップアドレスを使用して応答します。

No.	Time	Source	Destination	Protocol	Info
2	0.000992	<b>172.22.1.161</b>	<b>172.20.1.2</b>	<b>DNS</b>	<b>Standard query response</b> <b>A 172.20.1.10</b>

```
Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2 (172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035)
Domain Name System (response)
  [Request In: 1]
  [Time: 0.000992000 seconds]
  Transaction ID: 0x000c
  Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    server.example.com: type A, class IN
      Name: server.example.com
      Type: A (Host address)
      Class: IN (0x0001)
Answers
  server.example.com: type A, class IN, addr 172.20.1.10
    Name: server.example.com
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 1 hour
    Data length: 4
    Addr: 172.20.1.10
```

4. ASA が DNS 応答の宛先アドレスの変換を元に戻し、パケットをクライアントに転送します。DNS Doctoring がイネーブルになっている場合、応答に含まれる Addr は WWW サーバのリアルアドレスに書き換えられます。

```
No.      Time      Source      Destination      Protocol Info
2        0.001251  172.22.1.161  192.168.100.2    DNS      Standard query response
                                                A 192.168.100.10
```

```
Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 52985 (52985)
Domain Name System (response)
```

```
[Request In: 1]
[Time: 0.001251000 seconds]
Transaction ID: 0x000c
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  server.example.com: type A, class IN
    Name: server.example.com
    Type: A (Host address)
    Class: IN (0x0001)
```

#### Answers

```
  server.example.com: type A, class IN, addr 192.168.100.10
    Name: server.example.com
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 1 hour
    Data length: 4
    Addr: 192.168.100.10
  !--- 172.20.1.10 has been rewritten to be 192.168.100.10.
```

5. この時点で、クライアントは 192.168.100.10 の WWW サーバにアクセスしようとします。接続は成功します。クライアントとサーバが同じサブネット上にあるため、ASA ではトラフィックは何もキャプチャされません。

## 「dns」キーワードを使用した最終的な設定

これは、dns キーワードと 2 つの NAT インターフェイスを使用した DNS Doctoring を実行するための ASA の最終的な設定です。

### 最終的な ASA 7.2(1) の設定

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
  nameif outside
```

```

security-level 0
ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10
netmask 255.255.255.255 dns
!--- PAT and static NAT configuration. The DNS keyword
instructs !--- the security appliance to rewrite DNS
records related to this entry. access-group OUTSIDE in
interface outside
!--- The Access Control List (ACL) that permits HTTP
access !--- to the WWW server is applied to the outside
interface. route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! policy-map type inspect
dns MY_DNS_INSPECT_MAP
parameters
 message-length maximum 512
!--- DNS inspection map. policy-map global_policy class
inspection_default inspect ftp inspect h323 h225 inspect
h323 ras inspect rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp inspect dns
MY_DNS_INSPECT_MAP
!--- DNS inspection is enabled using the configured map.
inspect icmp policy-map type inspect dns

```

```
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:a4a38088109887c3ceb481efab3dcf32
: end
```

## 別のソリューション：ヘアピンング

### スタティック NAT によるヘアピンング

**注意：**スタティック NAT のヘアピンングはセキュリティ アプライアンスを通してクライアントと WWW サーバ間のすべてのトラフィックを送信 することを含みます。このソリューションを実装する前に、トラフィックの予想量とセキュリティ アプライアンスの能力を慎重に考慮してください。

ヘアピンングとは、トラフィックを到達したのと同じインターフェイスに戻すプロセスです。この機能は、セキュリティ アプライアンス ソフトウェア バージョン 7.0 で導入されています。7.2(1) よりも前のバージョンでは、ヘアピンングされるトラフィックの少なくとも 1 つのアーム (インバウンドまたはアウトバウンド) を暗号化する必要があります。7.2(1) 以降では、この条件は不要です。7.2(1) を使用する際には、インバウンドトラフィックとアウトバウンドトラフィックの両方とも暗号化されている必要はありません。

ヘアピンングをスタティック NAT 設定文と組み合わせると、DNS Doctoring と同じ効果が得られます。この方法では、DNS サーバからクライアントに返される DNS A レコードの内容は変更されません。その代わりに、このドキュメントで説明しているようなシナリオでヘアピンングを使用すると、クライアントは DNS サーバから返されるアドレス 172.20.1.10 を使用して接続できます。

ヘアピンングとスタティック NAT を使用して DNS Doctoring と同じ効果を得る場合の、関連する部分の設定は次のようになります。太字で示すコマンドについては、この出力の後で詳細に説明します。

```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
!--- Output suppressed. same-security-traffic permit intra-interface
!--- Enable hairpinning. global (outside) 1 interface !--- Global statement for client access to
the Internet. global (inside) 1 interface
!--- Global statment for hairpinned client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should be
natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real
address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255
!--- Static NAT statement mapping requests for the public IP address of !--- the WWW server that
appear on the inside interface to the WWW server's !--- real address of 192.168.100.10.
```

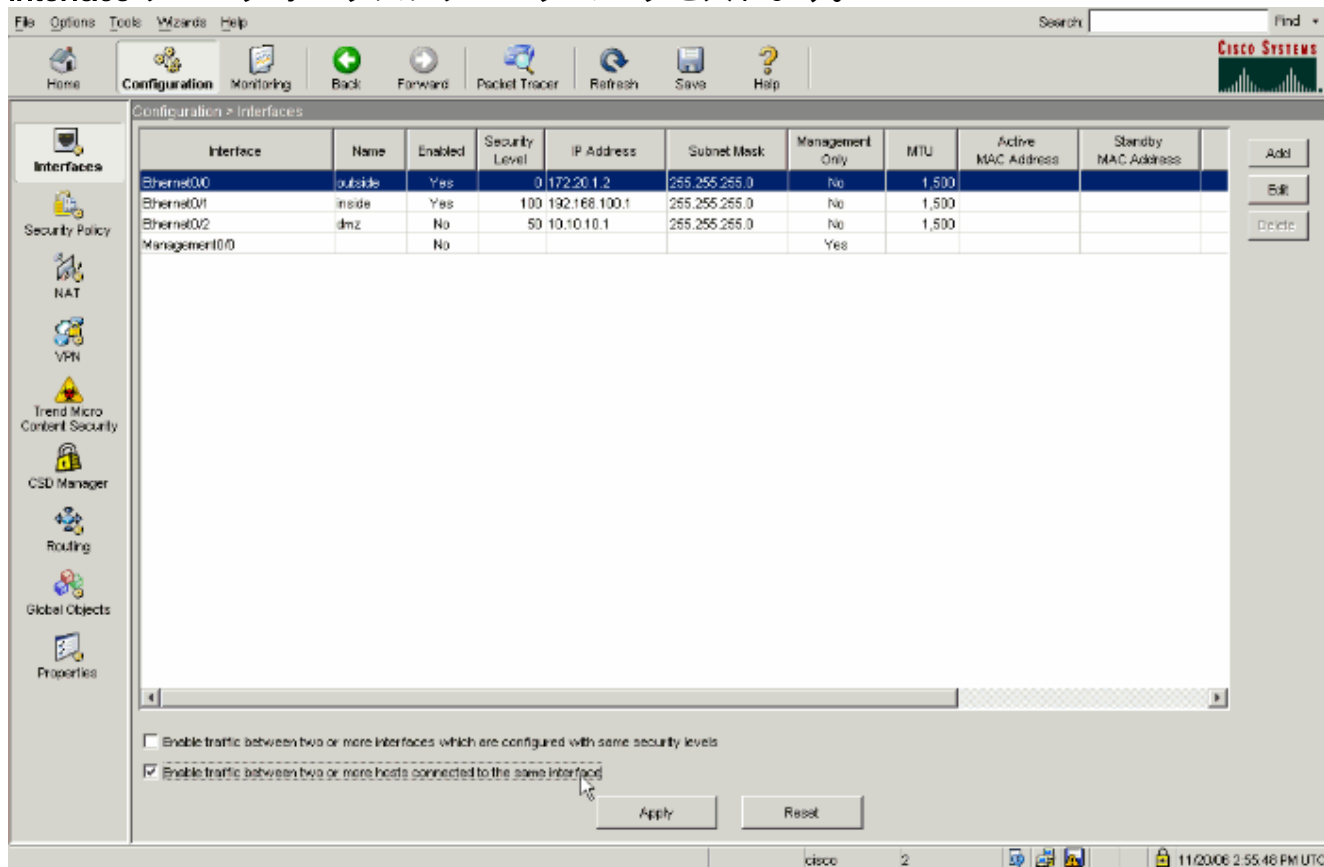
- **同じセキュリティトラフィック**—このコマンドはセキュリティ アプライアンスを通過することを同じセキュリティレベルのトラフィックが可能にします。 **permit intra-interface** キーワードは、same-security-traffic が同じインターフェイスで着発信できるようにするものであり、これによってヘアピンングがイネーブルになります。注: same-security-traffic [same-security-traffic](#)
- **グローバル な (中) 1 interface** —すべてのトラフィックはセキュリティ アプライアンスを

交差させる NAT を経る必要があります。このコマンドはキャンセルする hairpinned 内部インターフェイスと同時にトラフィックを有効にするために PAT を経るために内部インターフェイスに入るセキュリティ アプライアンスの内部インターフェイス アドレスを使用します。

- **172.20.1.10 静的な (中、中) 192.168.100.10 ネットマスク 255.255.255.255** —この静的 NAT エントリは WWW サーバのパブリック IP アドレスのための第 2 マッピングを作成します。しかし、1 番目のスタティック NAT エントリと異なり、ここではアドレス 172.20.1.10 がセキュリティ アプライアンスの inside インターフェイスにマップされます。これによって、セキュリティ アプライアンスが、inside インターフェイスで検出したこのアドレスについての要求に対応できるようになります。この後、これらの要求をアプライアンス自体を経由して WWW サーバの実アドレスにリダイレクトします。

ASDM でスタティック NAT を設定するには、次の手順を実行します。

1. **Configuration > Interfaces** へのナビゲート。
2. ウィンドウの下部にある **Enable traffic between two or more hosts connected to the same interface** チェック ボックスにチェック マークを入れます。



3. [Apply] をクリックします。
4. **Configuration > NAT** に移動し、**Add > Add Static NAT Rule...** の順に選択します。

Configuration > NAT

Addresses Services Global Pools

Real Source	Real Destination	Interface	Translated Address	DNS Rewrite	NAT Type
8.100.10	any	outside	172.20.1.10	No	Unit
network/24	any	outside	outside	No	Unit

Rule Flow Diagram

192.168.100.10 → inside → 192.168.100.10 → Static → 172.20.1.10 → outside → any

Device configuration loaded successfully. cisco 2 11/20/08 2:53:28 PM UTC

5. 新しいスタティック変換の設定を入力します。**Real Address** 領域に、WWW サーバの情報を入力します。**Static Translation** 領域に、WWW サーバにマッピングするアドレスとインターフェイスを入力します。この例では、inside インターフェイス上のホストが、マップアドレス 172.20.1.10 を介して WWW サーバにアクセスできるように inside インターフェイスが選択されています。



### Add Static NAT Rule

Real Address

Interface:

IP Address:

Netmask:

Static Translation

Interface:

IP Address:

Enable Port Address Translation (PAT)

Protocol:

Original Port:

Translated Port:

NAT Options...

OK Cancel Help

6. OK をクリックして、Add Static NAT Rule ウィンドウを閉じます。

7. 既存のダイナミック PAT トランスレーションを選択して、Edit をクリックします。

Configuration > NAT

Filter: --Select--

No	Type	Real		Translated		DNS Rewrite	Misc
		Source	Destination	Interface	Address		
-1	Static	192.168.100.10	any	outside	172.20.1.10	No	Unit
-2	Static	192.168.100.10	any	inside	172.20.1.10	No	Unit
-3	Dynamic	inside-network/24	any	outside	outside	No	Unit

Rule Flow Diagram

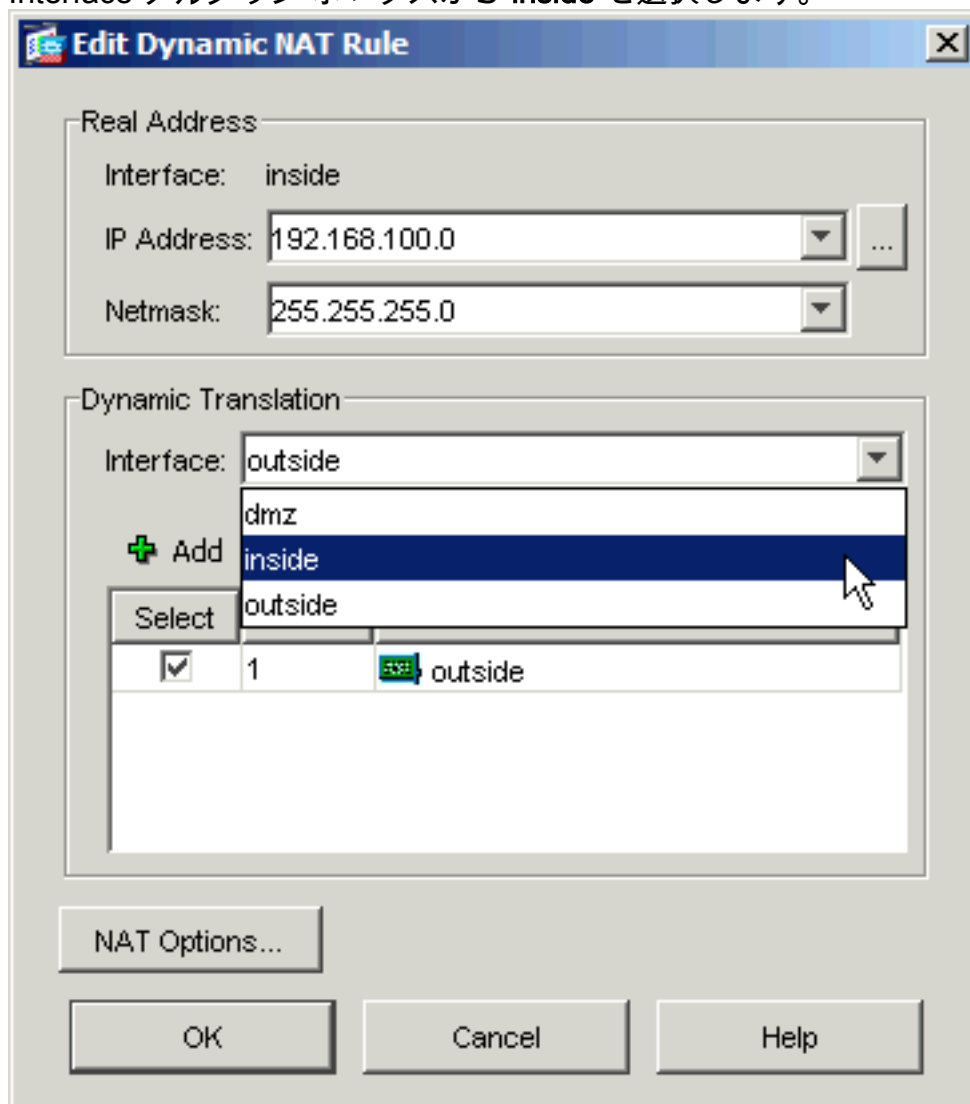
192.168.100.0/24 → inside-network/24 → inside → outside → outside → any

Enable traffic through the firewall without address translation

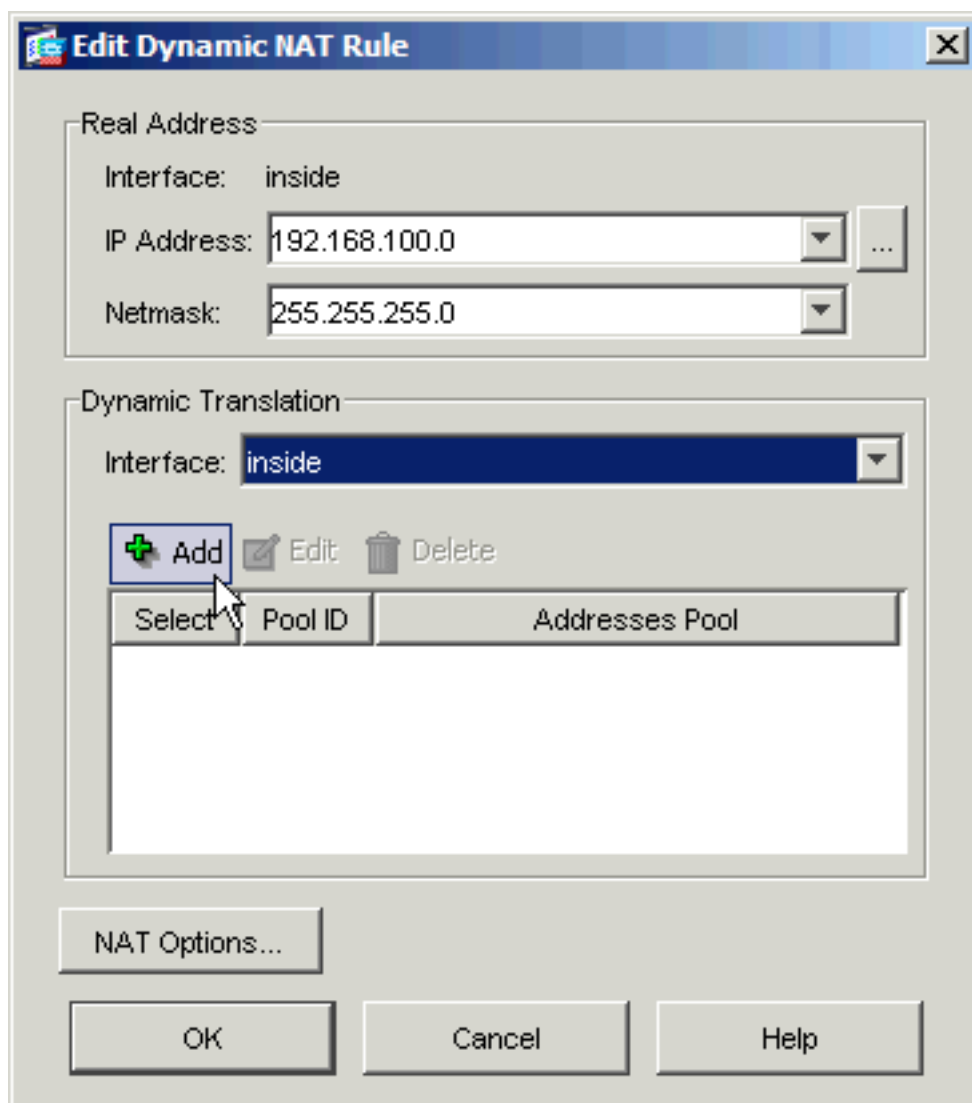
Apply Reset

Device configuration loaded successfully. cisco 2 11/20/06 9:02:58 PM UTC

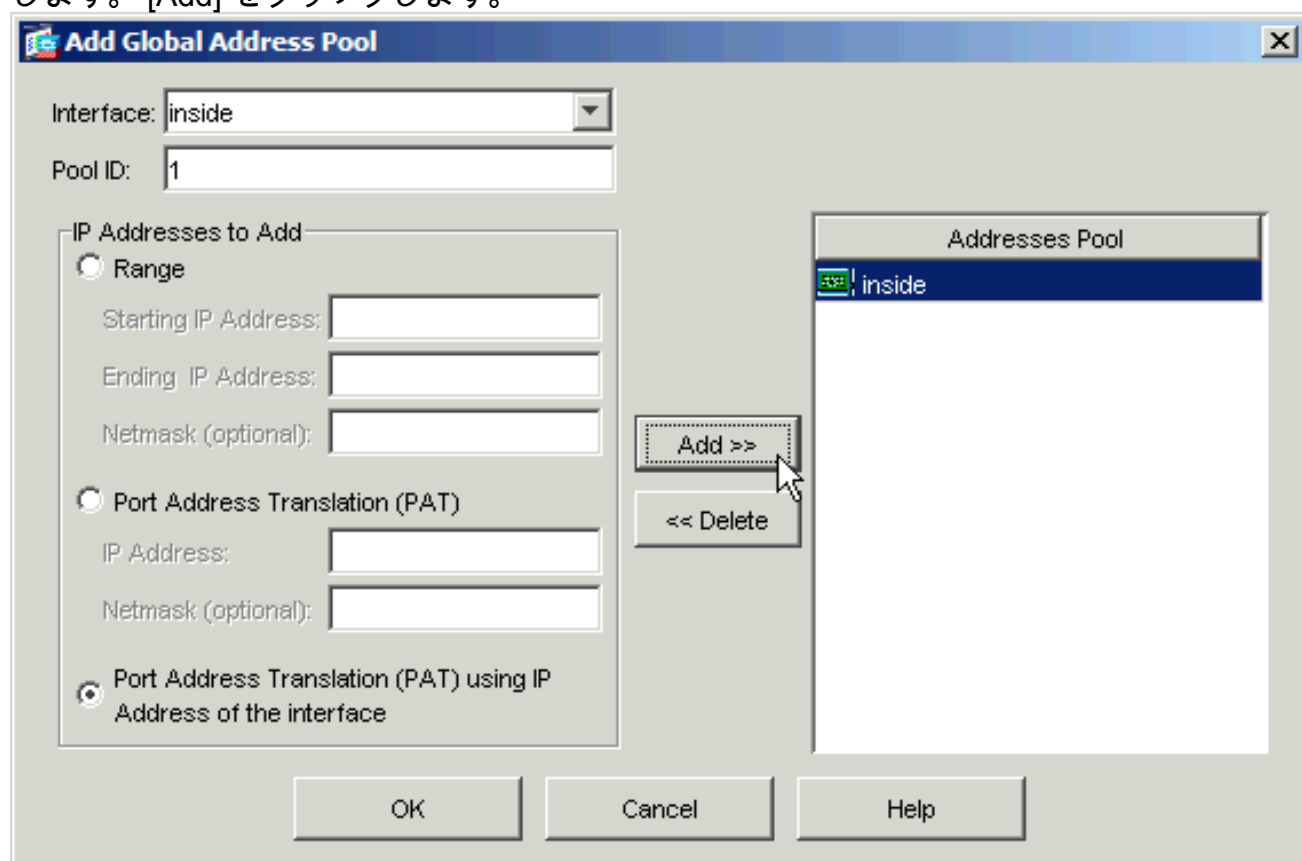
8. Interface プルダウン ボックスから **inside** を選択します。



9. [Add] をクリックします。



10. Port Address Translation (PAT) using IP address of the interface オプション ボタンを選択します。[Add] をクリックします。



11. **OK** をクリックして、Add Global Address Pool ウィンドウを閉じます。 **OK** をクリックして、Edit Dynamic NAT Rule ウィンドウを閉じます。 **Apply** をクリックして、セキュリティ アプライアンスに設定を送信します。

ヘアピンングが設定されている場合に発生する一連のイベントを次に示します。クライアントはすでに DNS サーバへ問い合わせを行い、WWW サーバのアドレスは 172.20.1.10 であるという応答を受信したと仮定します。

1. クライアントが 172.20.1.10 の WWW サーバに接続しようと試みます。

```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
!--- Output suppressed. same-security-traffic permit intra-interface
!--- Enable hairpinning. global (outside) 1 interface !--- Global statement for client
access to the Internet. global (inside) 1 interface
!--- Global statement for hairpinned client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should
be natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's
real address to a !--- public address on the outside interface. static (inside,inside)
172.20.1.10 192.168.100.10 netmask 255.255.255.255
!--- Static NAT statement mapping requests for the public IP address of !--- the WWW server
that appear on the inside interface to the WWW server's !--- real address of
192.168.100.10.
```

2. セキュリティ アプライアンスが要求を確認し、WWW サーバが 192.168.100.10 であることを認識します。

```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
!--- Output suppressed. same-security-traffic permit intra-interface
!--- Enable hairpinning. global (outside) 1 interface !--- Global statement for client
access to the Internet. global (inside) 1 interface
!--- Global statement for hairpinned client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should
be natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's
real address to a !--- public address on the outside interface. static (inside,inside)
172.20.1.10 192.168.100.10 netmask 255.255.255.255
!--- Static NAT statement mapping requests for the public IP address of !--- the WWW server
that appear on the inside interface to the WWW server's !--- real address of
192.168.100.10.
```

3. セキュリティ アプライアンスがクライアント用のダイナミック PAT トランスレーションを作成します。このときクライアントトラフィックの出典はセキュリティ アプライアンスの内部インターフェイスです: 192.168.100.1。

```
%ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to
inside:192.168.100.1/1026
```

4. セキュリティ アプライアンスがクライアントと WWW サーバの間の自身を経由する TCP 接続を確立します。カッコで囲まれた各ホストのマップアドレスに注意してください。

```
%ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012
(192.168.100.1/1026) to inside:192.168.100.10/80 (172.20.1.10/80)
```

5. セキュリティ アプライアンスで **show xlate** コマンドを実行すると、クライアントのトラフ

イックがセキュリティ アプライアンスを介して変換されていることが確認されます。

```
ciscoasa(config)#show xlate
3 in use, 9 most used
Global 172.20.1.10 Local 192.168.100.10
Global 172.20.1.10 Local 192.168.100.10
PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)
```

6. セキュリティ アプライアンスで **show conn** コマンドを実行すると、クライアントに代わって、セキュリティ アプライアンスと WWW サーバの間の接続が正しく行われていることを確認できます。カッコで囲まれたクライアントの WWW サーバの実アドレスに注意してください。

```
ciscoasa#show conn
TCP out 192.168.100.1(192.168.100.2):11019 in 192.168.100.10:80
idle 0:00:03 bytes 1120 flags UIOB
```

## ヘアピニングとスタティック NAT を使用した最終的な設定

これは、ヘアピニングとスタティック NAT を使用して 2 つの NAT インターフェイスで DNS Doctoring の効果を得る、ASA の最終的な設定です。

### 最終的な ASA 7.2(1) の設定

```
ciscoasa(config-if)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface
access-list OUTSIDE extended permit tcp any host
```

```
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface !--- Global statement for client access to the
Internet. global (inside) 1 interface !--- Global
statement for hairpinned client access through !--- the
security appliance. nat (inside) 1 192.168.100.0
255.255.255.0 !--- The NAT statement defines which
traffic should be natted. !--- The whole inside subnet
in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT
statement mapping the WWW server's real address to a
public !--- address on the outside interface. static
(inside,inside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 !--- Static NAT statement mapping
requests for the public IP address of the !--- WWW
server that appear on the inside interface to the WWW
server's real address !--- of 192.168.100.10. access-
group OUTSIDE in interface outside !--- The ACL that
permits HTTP access to the WWW server is applied !--- to
the outside interface. route outside 0.0.0.0 0.0.0.0
172.20.1.1 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth
0:05:00 absolute username cisco password
ffIRPGpDSOJh9YLq encrypted http server enable no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic !! policy-map type inspect dns
MY_DNS_INSPECT_MAP parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect ftp inspect h323 h225 inspect h323 ras inspect
rsh inspect rtsp inspect esmtp inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:7c9b4e3aff085ba90ee194e079111e1d
: end
```

注: このビデオを、ヘアピニングが使用できる異なるシナリオに関する詳細については[ヘアピニング ASA \(登録ユーザのみ\)](#)、[on Cisco](#) 参照して下さい。

## [DNS インспекションの設定](#)

( DNS インспекションを以前にディセーブルにしている場合 ) DNS インспекションをイネーブルにするには、次の手順を実行します。この例では、DNS インспекションをデフォルトのグローバル インспекション ポリシーに追加しています。このポリシーは、ASA のデフォルト設定から作業を開始した場合と同様に、**service-policy** コマンドによってグローバルに適用されます。サービス ポリシーおよびインспекションについての詳細は、『[モジュラ ポリシーフレームワークの使用](#)』を参照してください。

1. DNS 用のインスペクション ポリシー マップを作成します。

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
```

2. policy-map 設定モードから、インスペクション エンジンのパラメータを指定するためにパラメータ設定モードに入ります。

```
ciscoasa(config-pmap)#parameters
```

3. policy-map パラメータ設定モードで、DNS メッセージの最大長を 512 に設定します。

```
ciscoasa(config-pmap-p)#message-length maximum 512
```

4. policy-map パラメータ設定モードと policy-map 設定モードを終了します。

```
ciscoasa(config-pmap-p)#exit
```

```
ciscoasa(config-pmap)#exit
```

5. インスペクション ポリシーマップが正しく作成されたことを確認します。

```
ciscoasa(config)#show run policy-map type inspect dns
```

```
!
```

```
policy-map type inspect dns MY_DNS_INSPECT_MAP
```

```
parameters
```

```
message-length maximum 512
```

```
!
```

6. global\_policy の policy-map 設定モードに入ります。

```
ciscoasa(config)#policy-map global_policy
```

```
ciscoasa(config-pmap)#
```

7. policy-map 設定モードで、デフォルトのレイヤ 3/4 クラス マップ inspection\_default を指定します。

```
ciscoasa(config-pmap)#class inspection_default
```

```
ciscoasa(config-pmap-c)#
```

8. policy-map クラス設定モードで、手順 1 ~ 3 で作成したインスペクション ポリシー マップを使用して DNS を検査するように指定します。

```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```

9. policy-map クラス設定モードと policy-map 設定モードを終了します。

```
ciscoasa(config-pmap-c)#exit
```

```
ciscoasa(config-pmap)#exit
```

10. global\_policy ポリシーマップが正しく設定されたことを確認します。

```
ciscoasa(config)#show run policy-map
```

```
!
```

```
!--- The configured DNS inspection policy map. policy-map type inspect dns
```

```
MY_DNS_INSPECT_MAP parameters message-length maximum 512 policy-map global_policy class
```

```
inspection_default inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp
```

```
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip
```

```
inspect netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
```

```
!--- DNS application inspection enabled. !
```

11. global\_policy が service-policy によってグローバルに適用されることを確認します。

```
ciscoasa(config)#show run service-policy
```

```
service-policy global_policy global
```

## スプリット DNS の設定

split-dns コマンドをグループ ポリシー コンフィギュレーション モードで発行して、ドメインのリストを入力し、スプリット トンネルを経由して解決されるようにします。 リストを削除するには、このコマンドの **no** の形式を使用します。

スプリット トンネリングのドメイン リストがない場合は、ユーザはデフォルトのグループ ポリシーにあるものを継承します。スプリット トンネリングのドメイン リストを継承しないようにするには、**split-dns none** コマンドを発行します。

ドメイン リスト内の各エントリを分けるには、スペースを1つ使用します。エントリの数に制限はありませんが、全体の文字列は255文字を超えることはできません。使用できる文字は、英数字、ハイフン (-)、ピリオド (.) だけです。**no split-dns** コマンドを引数なしで使用すると、現在の値がすべて削除されます。これには、**split-dns none** コマンドを発行した際に作成されたヌルの値も含まれます。

この例では、Domain1、Domain2、Domain3、および Domain4 というドメインを設定して、FirstGroup という名前のグループ ポリシーに対するスプリット トンネルによって解決されるようにしています。

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

## 確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) ( OIT ) ( [登録ユーザ専用](#) ) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

## DNS トラフィックのキャプチャ

セキュリティ アプライアンスが DNS レコードを正しく書き換えているかどうかを確認する方法の1つは、上の例で説明したように、該当するパケットをキャプチャすることです。ASA でトラフィックをキャプチャするには、次の手順を実行します。

1. 作成するキャプチャ インスタンスごとにアクセス リストを作成します。キャプチャするトラフィックが ACL で指定されている必要があります。この例では、2 つ ACL を作成します。  
。outside インターフェイスのトラフィックに対する ACL :

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

inside インターフェイスのトラフィックに対する ACL :

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

2. キャプチャ インスタンスを作成します。

```
ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface outside
!--- This capture collects traffic on the outside interface that matches !--- the ACL
DNSOUTCAP. ciscoasa#capture DNSINSIDE access-list DNSINCAP interface inside
!--- This capture collects traffic on the inside interface that matches !--- the ACL
DNSINCAP.
```

3. キャプチャを表示します。DNS トラフィックが通過した後、この例のキャプチャは次のようになります。

```
ciscoasa#show capture DNSOUTSIDE
2 packets captured
  1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53:  udp 36
  2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025:  udp 93
```



```
2 packets shown
ciscoasa#show capture DNSINSIDE
2 packets captured
  1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53:  udp 36
  2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225:  udp 93
2 packets shown
```

4. ( オプション ) 他のアプリケーションで分析できるように pcap 形式でキャプチャを TFTP サーバにコピーします。pcap 形式を解析できるアプリケーションでは、DNS A レコードに含まれる名前や IP アドレスなどの詳細情報も表示できます。

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

### DNS 書き換えが実行されない

セキュリティ アプライアンスで DNS インспекションが設定されていることを確認してください。「[DNS インспекションの設定](#)」セクションを参照してください。

### 変換の作成に失敗する

クライアントと WWW サーバの間で接続を確立できない場合は、NAT の設定ミスが原因である可能性があります。セキュリティ アプライアンスのログを開いて、プロトコルがセキュリティ アプライアンスを介して変換を作成することに失敗したことを示すメッセージがないかどうかを確認してください。そのようなメッセージがある場合は、適切なトラフィックに対して NAT が設定されていて、アドレスに誤りがないことを確認してください。

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

次に xlate エントリを削除し、このエラーを解決するために NAT 文を取除き、再適用して下さい。

### UDP DNS 応答を廃棄して下さい

DNS パケット破棄によるこのエラーメッセージを受け取ることは可能性のあるです:

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

この問題を解決するために 512-65535 間の DNS パケット 長を増加して下さい。

例 :

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

## [関連情報](#)

- [Cisco PIX Firewall ソフトウェア](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [セキュリティ製品フィールド通知](#)
- [Request for Comments \( RFC \)](#)
- [ヘアピニング on Cisco ASA](#)
- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)