ASA リリース 9.x で 3 つの NAT インターフェイス用に DNS Doctoring を設定する

目次

概要

この資料は Domain Name System （ DNS ）を行うために設定 例を提供したものです適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) 使用反対しましたり/オート ネットワーク アドレス変換 (NAT) 文その ASA 5500-X シリーズで治療します。 DNS Doctoring により、セキュリティ アプライアンスが DNS A レコードを書き換えられるようになります。

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。

前提条件

要件

Cisco はセキュリティ アプライアンス モデルで治療する DNS を行うために DNS インスペクションが有効に する必要があることを示します。 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。

- 完了する設定に基づいてオブジェクト/オート Nat コマンド (DNS リライト) の使用と DNS レコードを変換します。 変換は DNS 応答の A レコードだけに適用されます。 従ってポインタ (PTR) レコードを要求する逆ルックアップは DNS 書き直しから影響を受けません。 リバース DNS ルックアップのための DNS PTR レコードのバージョン ASA 9.0(1) およびそれ以降、変換、IPv6 NAT、および NAT64 IPv4 NAT を場合の NAT ルールのために有効に なる DNS インスペクションと使用する。**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)。 再組立てはパケット 長がより少しであることを確認するためにより最大長必要に応じて設定した実行された。 最大長を超えるパケットは廃棄されます。**注:** 最大長 オプションなしで **Inspect dns** コマンドを入力する場合、DNS パケット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

この文書に記載されている情報は ASA 5500-X シリーズ セキュリティ アプライアンス モデルに、バージョン 9.x 基づいています。

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。

関連製品

この設定も Cisco ASA 5500 シリーズ セキュリティ アプライアンス モデルとバージョン 8.4 または それ 以降使用することができます。

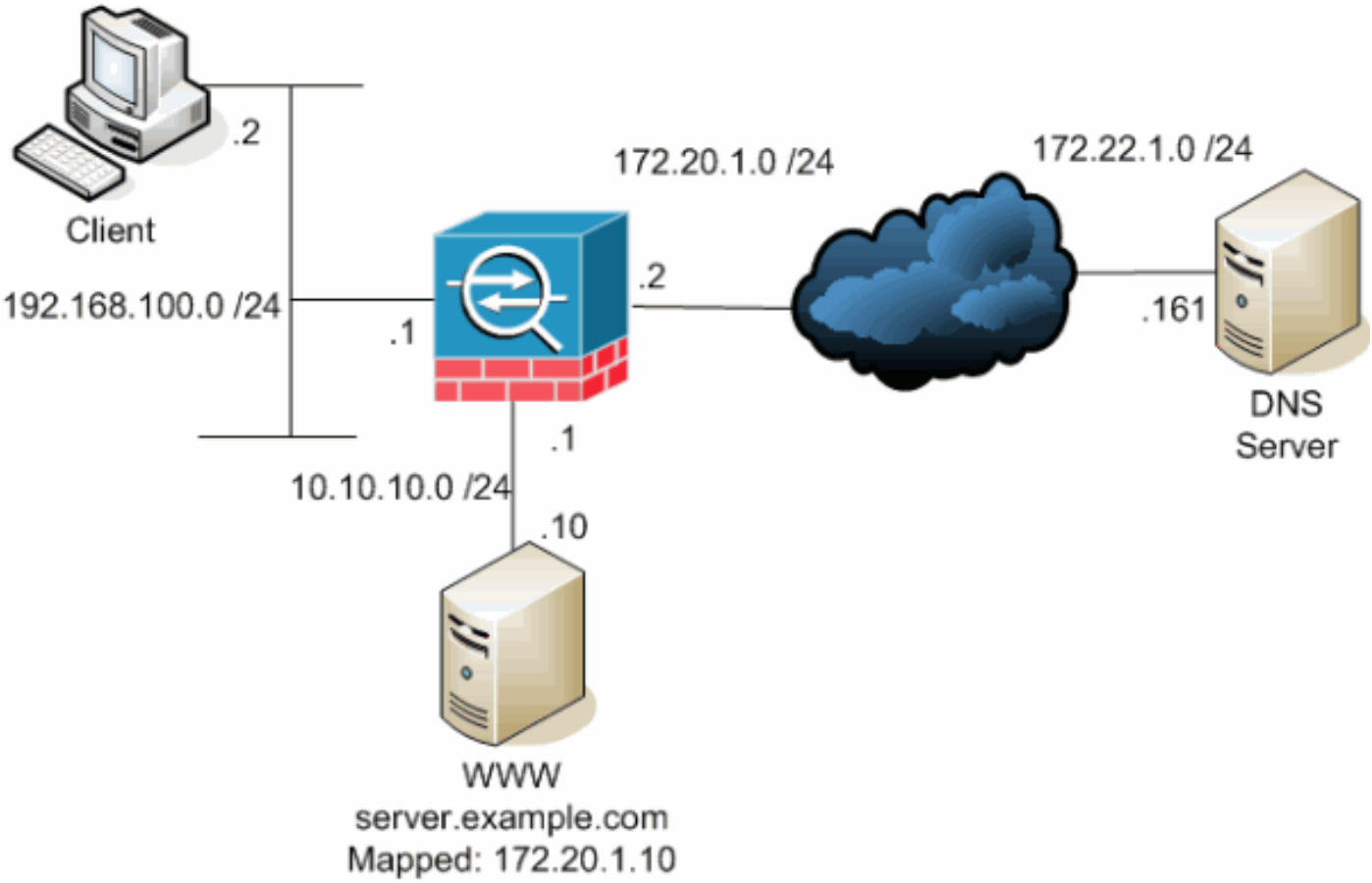
注: ASDM の設定はバージョン 7.x だけに適用できます。

背景説明

典型的な DNS 交換では、クライアントは DNSサーバにそのホストの IP アドレスを判別するために URL かホスト名を送信 します。 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： 3 つの NAT インターフェイス-の中、外部、DMZ

トポロジ



この図は、この状況の例です。 この場合、192.168.100.2 のクライアントは 10.10.10.10 で WWW サーバにアクセスするために **server.example.com** URL を使用したいと思います。 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

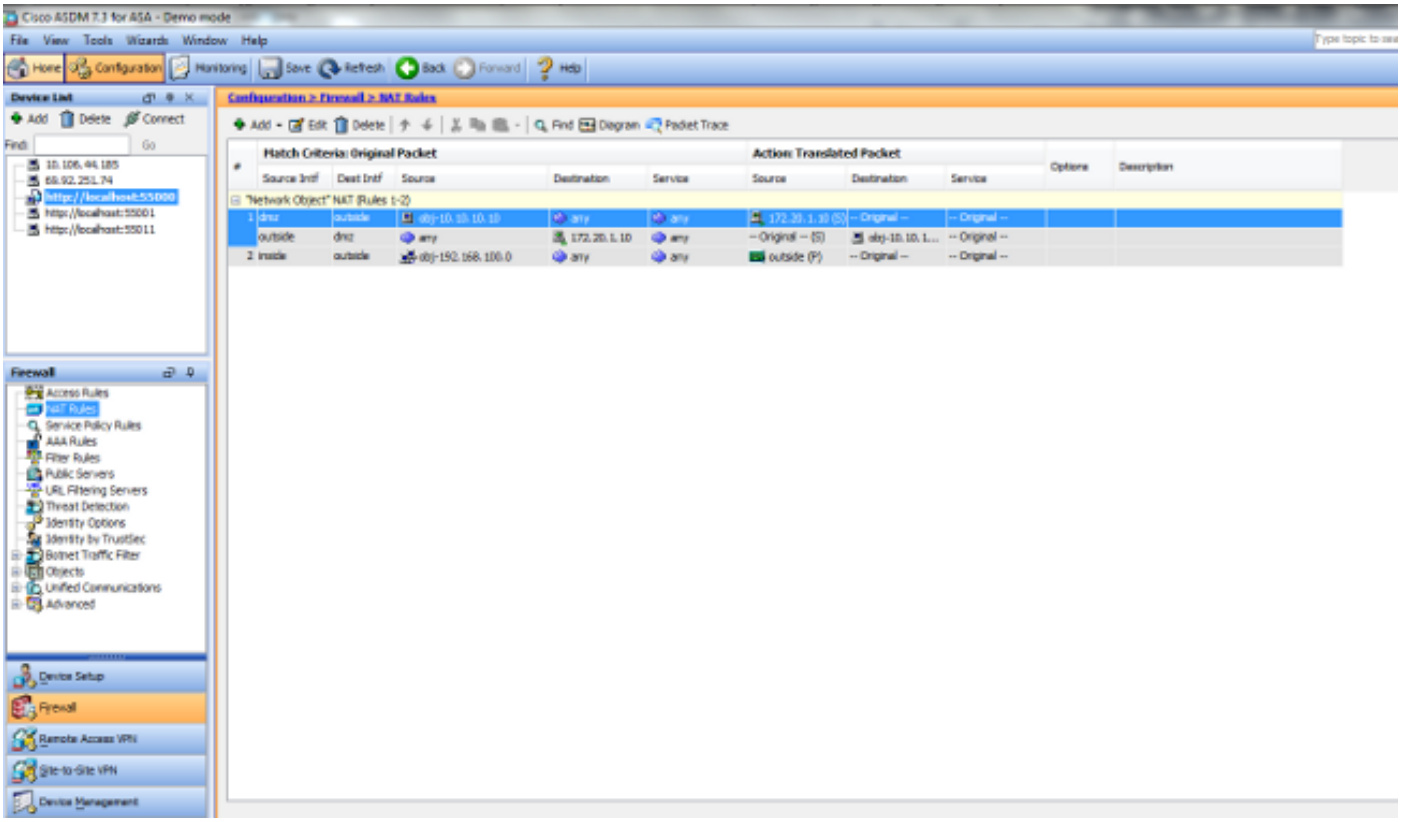
ドレスと名前のマッピングが含まれています。

問題： クライアントは WWW サーバにアクセスできません

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、WWW サーバのパブリック アドレス（172.20.1.10）を含む A レコードをクライアントが受信するためです。 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と、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。

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.
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: 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
   1 0.000000 **172.20.1.2** 172.22.1.161 DNS Standard query A server.example.com

   Frame 1 (78 bytes on wire, 78 bytes captured)
   Ethernet II, Src: Cisco_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: 1044 (1044), 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)
```

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 0.005005 172.22.1.161 172.20.1.2 DNS Standard query response
A 172.20.1.10

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: 1044 (1044)
Domain Name System (response)
[Request In: 1]
[Time: 0.005005000 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
```

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ない場合、応答に含まれる Addr は WWW サーバのマップ アドレスのままです。

```
No.     Time      Source         Destination
Protocol Info
2 0.005264 172.22.1.161 192.168.100.2 DNS Standard query response
A 172.20.1.10

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: 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 で WWW サーバにアクセスすることを試みます。 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 dmz 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 モデルは「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えることができます: クライアントは接続するためにセクション WWW サーバに」アクセスできません。 この場合有効に なる DNS 治療とセキュリティ アプライアンス モデルは 172.20.1.10 の代りに 10.10.10.10 にクライアントを指示するためにレコードを書き換えます。 DNS 治療はスタティック NAT 文 (バージョン 8.2 および それ以前) に **dns** キーワードを追加したりまたは (バージョン 8.3 および それ 以降) 反対したり/オート NAT 文とき有効に なります。

バージョン 8.2 および それ 以前

これは治療するバージョン 8.2 および それ 以前のための **dns** キーワードおよび 3 つの NAT インターフェイスと DNS を行う ASA の最終コンフィギュレーションです。

```
ciscoasa#show running-config
: Saved
:
```

```
ASA Version 8.2.x
!
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
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
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

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 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,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0
static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

access-group OUTSIDE in interface outside

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:d6637819c6ea981daf20d8c7aa8ca256
: end
```

バージョン 8.3 および それ 以降

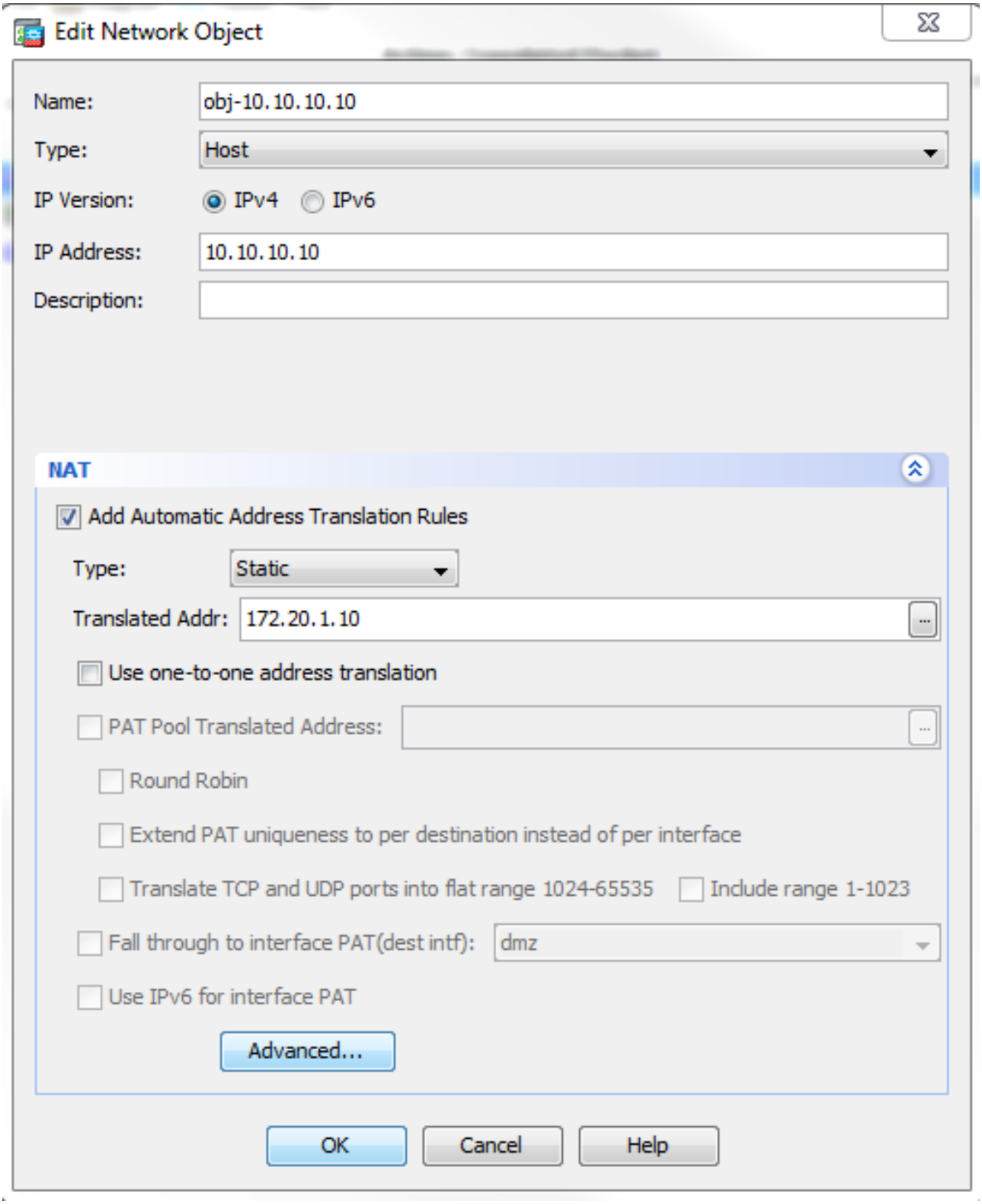
```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

ASDM の設定

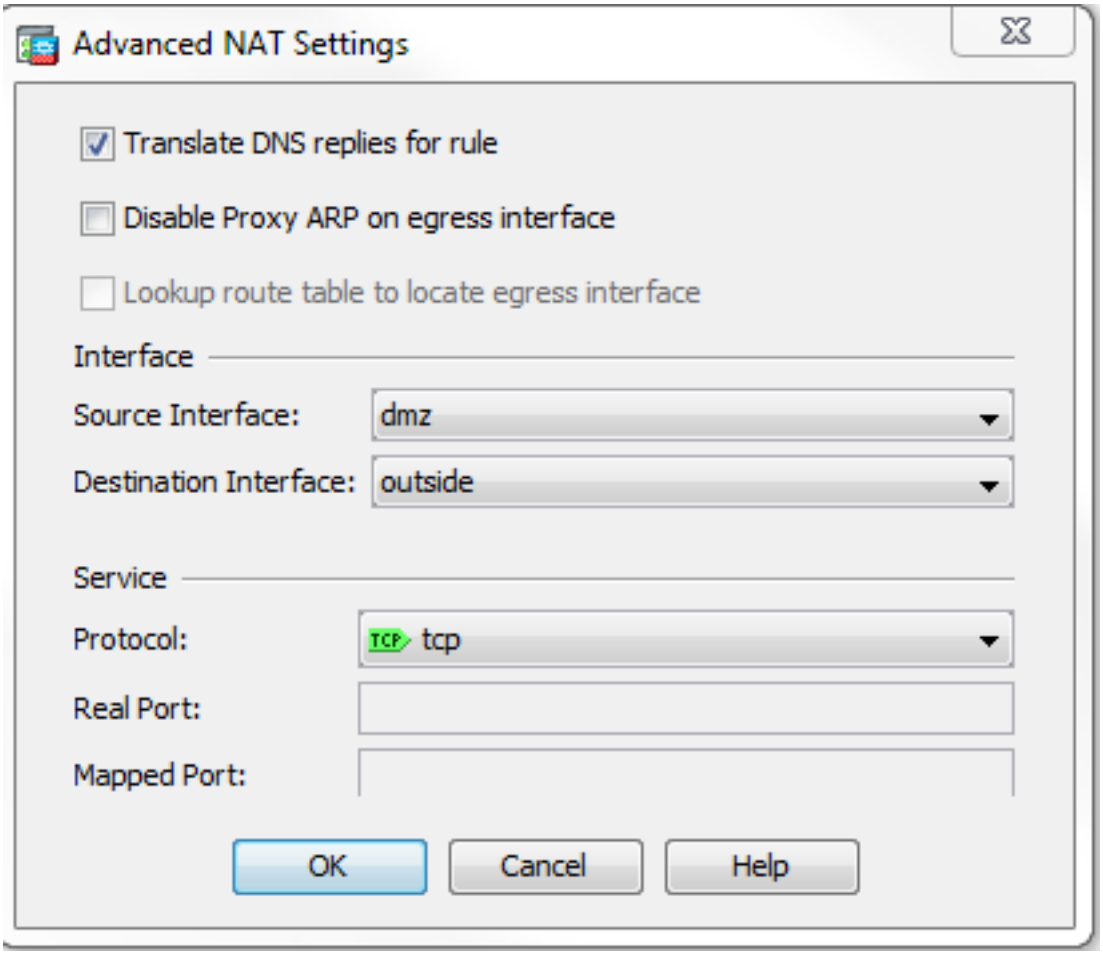
ASDM で DNS Doctoring を設定するには、次の手順を実行します。

1. **> NAT ルール**『Configuration』 を選択 し、修正されるオブジェクト/オート ルールを選択して下さい。 [Edit] をクリックします。
2. 『Advanced』 をクリック して下さい

...



3. **ルール** チェックボックスが**あるように変換 DNS 応答を**確認して下さい。



4. NAT Options ウィンドウを残すために『OK』 をクリック して下さい。
5. 編集オブジェクト/自動 NAT ルール ウィンドウを残すために『OK』 をクリック して下さい。
6. セキュリティ アプライアンス モデルに設定を送信 するために『Apply』 をクリック して下さい。

確認

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 **172.20.1.2** 172.22.1.161 DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_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 **172.22.1.161 172.20.1.2 DNS Standard query response**
A 172.20.1.10

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
   6 2.507191 **172.22.1.161 192.168.100.2 DNS Standard query response A 10.10.10.10**

   Frame 6 (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: 50752 (50752)
   Domain Name System (response)
   [Request In: 5]
   [Time: 0.002182000 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 10.10.10.10
   Name: server.example.com
   Type: A (Host address)
   Class: IN (0x0001)
   Time to live: 1 hour
   Data length: 4
   Addr: 10.10.10.10
5. この時点で、クライアントは 10.10.10.10 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。

「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 3 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。

```
ciscoasa# sh running-config
: Saved
:
: Serial Number: JMX1425L48B
: Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(5)4
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
```

```
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10 dns
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
```

```
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 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 ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3a8e3009aa3db1d6dba143abf25ee408
: end
```

別のソリューション： 宛先 NAT

宛先 NAT は DNS Doctoring の代替策として使用できます。 送信先 NAT の使用はこの場合静的な オブジェクト/オート NAT 変換が内部の WWW サーバ パブリックアドレスと DMZ の実 アドレスの間で作成されることを必要とします。 宛先 NAT の場合、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。 このドキュメントで説明されているような

シナリオで宛先 NAT を使用すると、クライアントは DNS サーバから返されるパブリック IP アドレス 172.20.1.10 を使用して WWW サーバに接続できます。 静的 な オブジェクト/オート変換はセキュリティ アプライアンス モデルが 172.20.1.10 からの 10.10.10.10 への宛先アドレスを変換するようにします。 宛先 NAT を使用する場合の設定の関連部分を次に示します。

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- The nat and global commands allow
!--- clients access to the Internet.

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

object network obj-10.10.10.10-1
host 10.10.10.10
nat (dmz,inside) static 172.20.1.10
```

手動/二度 NAT の設定例と実現する送信先 NAT

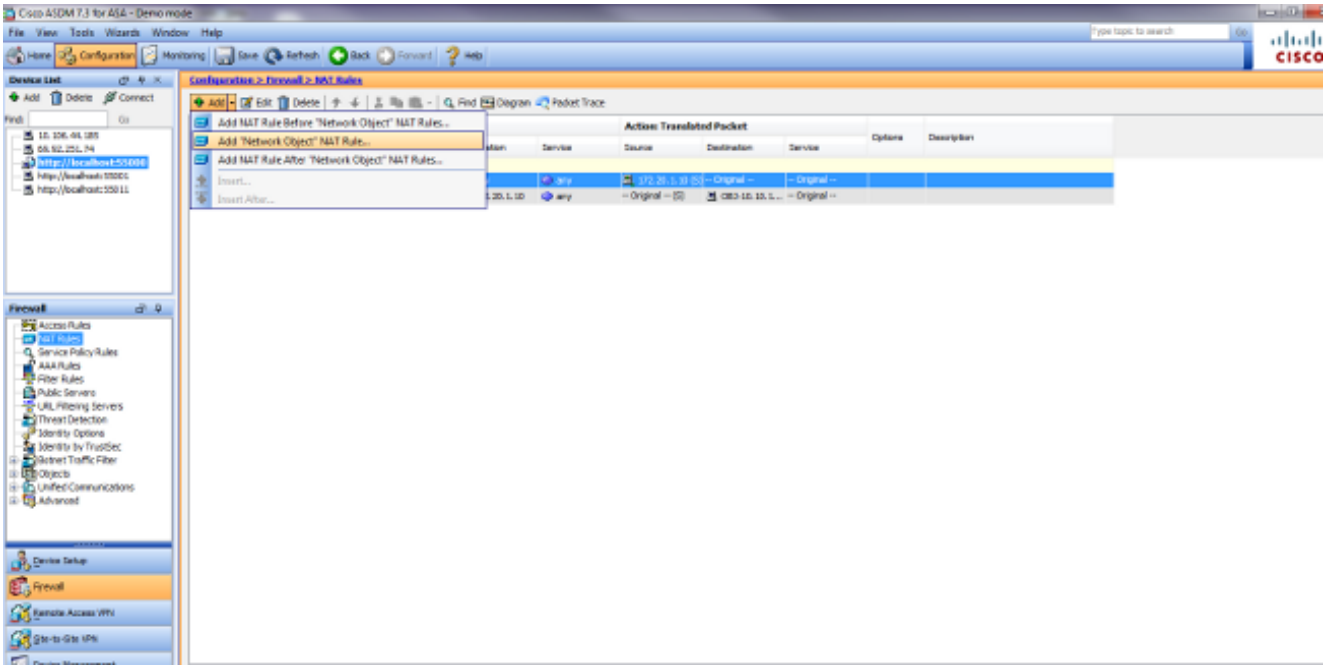
```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10

object network obj-172.20.1.10
host 172.20.1.10

nat (inside,dmz) source dynamic obj-192.168.100.0 interface
destination static obj-172.20.1.10 obj-10.10.10.10

!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.

access-group OUTSIDE in interface outside
```

```
!--- Output suppressed.
```

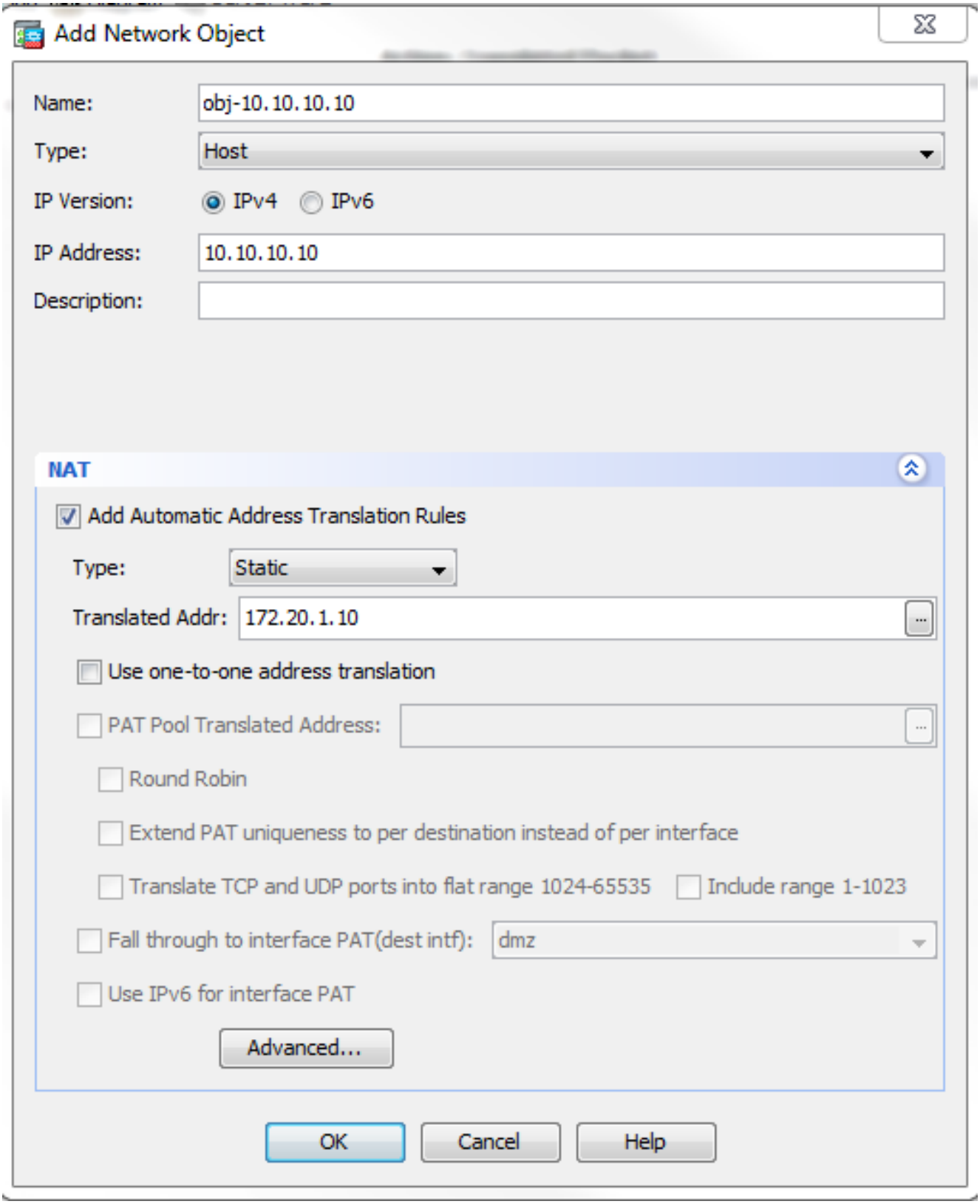
ASDM で宛先 NAT を設定するには、次の手順を実行します。

1. **> NAT ルール**『Configuration』 を選択 し、『Add』 を選択 して下さい **> Add 「ネットワーク オブジェクト」NAT ルールを**

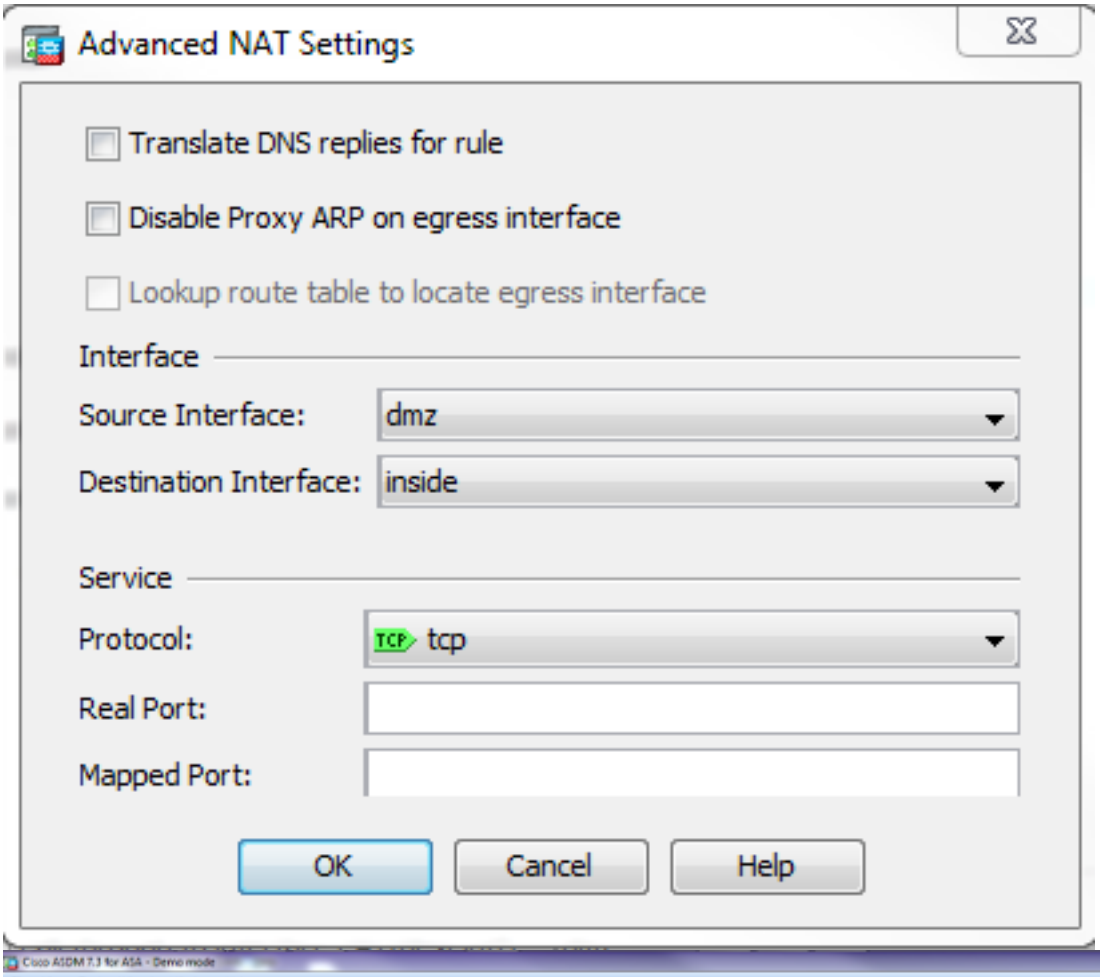
   ....

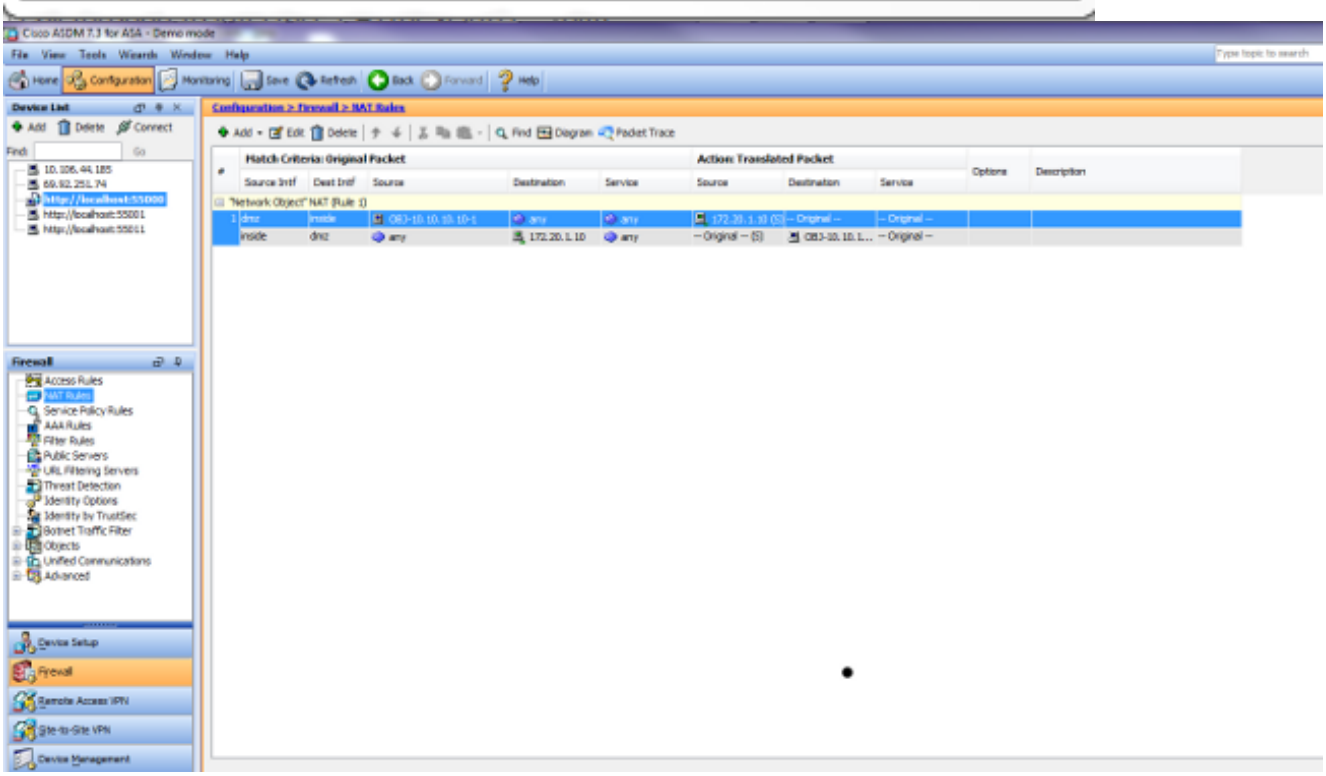


2. 新しいスタティック変換の設定を入力します。 Name フィールドでは、**obj-10.10.10.10 を**入力して下さい。IP Address フィールドでは、WWW サーバのIPアドレスのアドレスを入力して下さい。型ドロップダウン リストから、**スタティックを**選択して下さい。変換されたアドレス· フィールドでは、アドレスを入力し、WWW サーバをにマッピング したいと思うことインターフェイスさせて下さい。[Advanced] をクリックします。



ソースインターフェイス ドロップダウン リストで、**dmz** を選択して下さい。デスティネーションインターフェイス ドロップダウン リストで、**中**選択して下さい。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。

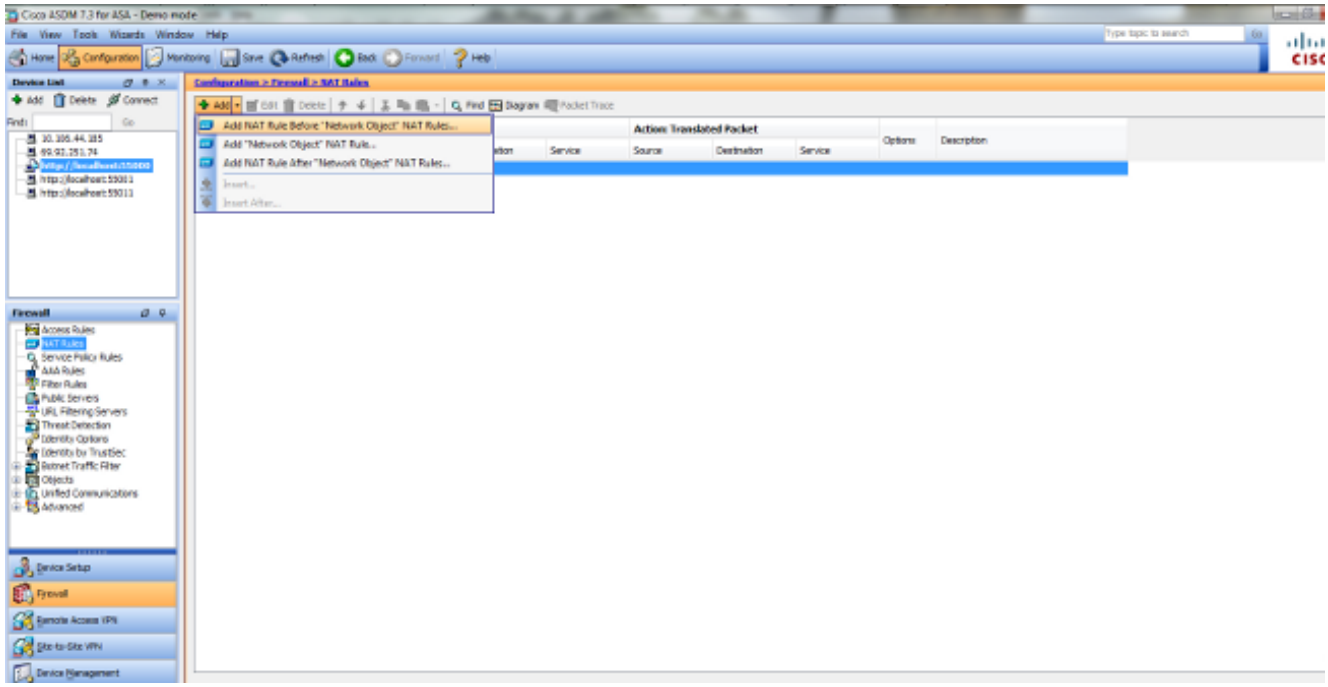




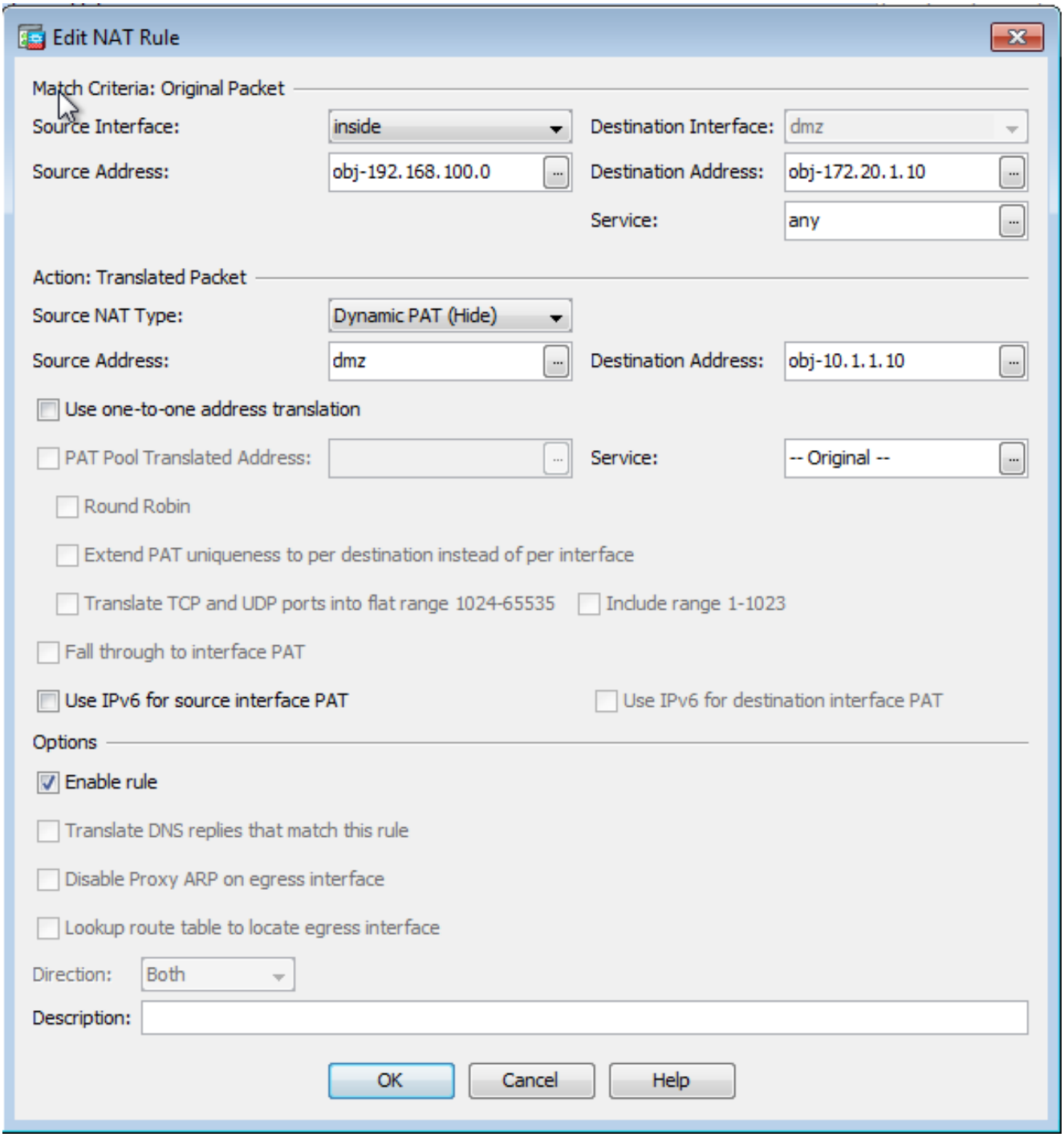
追加オブジェクト/自動 NAT ルール ウィンドウを残すために『OK』 をクリック して下さい。セキュリティ アプライアンス モデルに設定を送信 するために『Apply』 をクリック して下さい。

手動/二度 NAT および ASDM の代替方式

1. **「ネットワーク オブジェクト」NAT ルール....前に > NAT ルール**『Configuration』 を選択し、**> Add NAT ルールを**『Add』 を選択 して下さい



2. 手動のための設定を記入して下さい/二度変換をネットワークアドレス交換して下さい。 ソースインターフェイス ドロップダウン リストで、**中**選択して下さい。デスティネーション インターフェイス ドロップダウン リストで、**dmz を**選択して下さい。送信元アドレス フィールドでは、内部ネットワーク オブジェクト（obj-192.168.100.0）を入力して下さい。宛先 アドレス フィールドでは、変換された DMZ サーバIP オブジェクトを入力して下さい（172.20.1.10）。出典 NAT 型ドロップダウン リストで、**ダイナミック PAT（非表示）を**選択して下さい。送信元アドレス[処理: 変換されたパケット セクション]フィールドは、**dmz を**入力します。宛先アドレス[処理: 変換されたパケット セクション]フィールドは、DMZ サーバ実質 IP オブジェクト（obj-10.10.10.10）を入力します。



3. 追加手動/二度 NAT ルール ウィンドウを残すために『OK』 をクリック して下さい。
4. セキュリティ アプライアンス モデルに設定を送信 するために『Apply』 をクリック して下さい。

宛先 NAT 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。`%ASA-7-609001: Built local-host inside:192.168.100.2`
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 10.10.10.10 であることを認識します。`%ASA-7-609001: Built local-host dmz:10.10.10.10`
3. 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 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 outbound TCP connection 67956 for dmz:10.10.10.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001 (192.168.100.2/11001)`
4. 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

ィ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。 この例では、最初のスタティック変換が使用されています。ciscoasa#**show xlate**
3 in use, 9 most used
Global 192.168.100.0 Local 192.168.100.0
Global 172.20.1.10 Local 10.10.10.10
Global 172.20.1.10 Local 10.10.10.10

5. 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、クライアントと WWW サーバの間の接続がセキュリティ アプライアンスを介して成功したことが確認されます。 カッコで囲まれた WWW サーバのリアル アドレスに注意してください。ciscoasa#**show conn**
TCP out 172.20.1.10**(10.10.10.10)**:80 in 192.168.100.2:11001
idle 0:01:38 bytes 1486 flags UIO

宛先 NAT を使用した最終的な設定

これは、宛先 NAT と 3 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。

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
```

```
 host 10.10.10.10
object network obj-10.10.10.10-1
 host 10.10.10.10
object network obj-172.20.1.10
 host 172.20.1.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
 nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
```

```
 class inspection_default
 inspect dns preset_dns_map
 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 ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
: end
```

設定

以前、DNS インスペクションをディセーブルにしている場合、DNS インスペク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 インスペクションをデフォルトのグローバル インスペクション 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。

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. ポリシーマップコンフィギュレーション モードから、インスペクション エンジンのためのパラメータを規定 するためにパラメータ構成 モードを開始して下さい。`ciscoasa(config-pmap)#`**`parameters`**
3. policy-map パラメータ構成 モードでは、512 であるために DNS メッセージのための最大メッセージの長さを規定 して下さい。`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 クラスコンフィギュレーションモードでは、DNS が点検する必要があること規定 するために作成されるステップでインスペクション ポリシーマップを 1-3 使用して下さい。`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`

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：`access-list DNSOUTCAP extended`

```
permit ip host 172.22.1.161 host
172.20.1.2

!--- All traffic between the DNS server and the ASA.

access-list DNSOUTCAP extended permit ip host 172.20.1.2 host
172.22.1.161

!--- All traffic between the ASA and the DNS server.
```

inside インターフェイスのトラフィックに対する ACL：`access-list DNSINCAP extended`

```
permit ip host 192.168.100.2 host
172.22.1.161

!--- All traffic between the client and the DNS server.

access-list DNSINCAP extended permit ip host 172.22.1.161 host
192.168.100.2

!--- All traffic between the DNS server and the client.
```

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 インスペクションが設定されていることを確認してください。

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。

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst inside:192.168.100.10/80
```

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。

関連情報

- Cisco ASA 5500-x コンフィギュレーション ガイド
- Cisco ASA 5500-x シリーズ コマンドレファレンス
- セキュリティ製品フィールド通知
- Request for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems