

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

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[背景説明](#)

[シナリオ：3つのNATインターフェイス：内部、外部、DMZ](#)

[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](#)

[「dns」キーワードを使用した DNS Doctoring](#)

[バージョン8.2以前](#)

[バージョン8.3以降](#)

[確認](#)

[「dns」キーワードを使用した最終的な設定](#)

[別のソリューション：宛先 NAT](#)

[宛先 NAT を使用した最終的な設定](#)

[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](#)

[関連情報](#)

概要

このドキュメントでは、ASA 5500-X シリーズ適応型セキュリティ アプライアンス (ASA) でドメイン 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 は、オブジェクト/自動ネットワーク アドレス変換 (NAT) ステートメントを使用します。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。

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有効にする必要があるとシスコは述べています。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。

- object/auto NATコマンド（DNS書き換え）を使用して完了した設定に基づいて、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。したがって、ポインタ(PTR)レコードを要求する逆引きは、DNS書き換えによる影響を受けません。バージョン ASA 9.0(1)以降では、NATルールに対するDNSインスペクションが有効になっているIPv4 NAT、IPv6 NAT、およびNAT64を使用する場合の、逆DNSルックアップ用のDNS PTRレコードのこの変換がエントリにのみ変換されます。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 書き換えはステータック 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）。再構成は、パケット長が設定された最大長よりも短いことを確認するために、必要に応じて実行されます。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inspect dnsコマンドを入力すると、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

このドキュメントの情報は、ASA 5500-Xシリーズセキュリティアプライアンスバージョン9.x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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、Cisco ASA 5500シリーズセキュリティアプライアンスバージョン8.4以降でも使用できます。

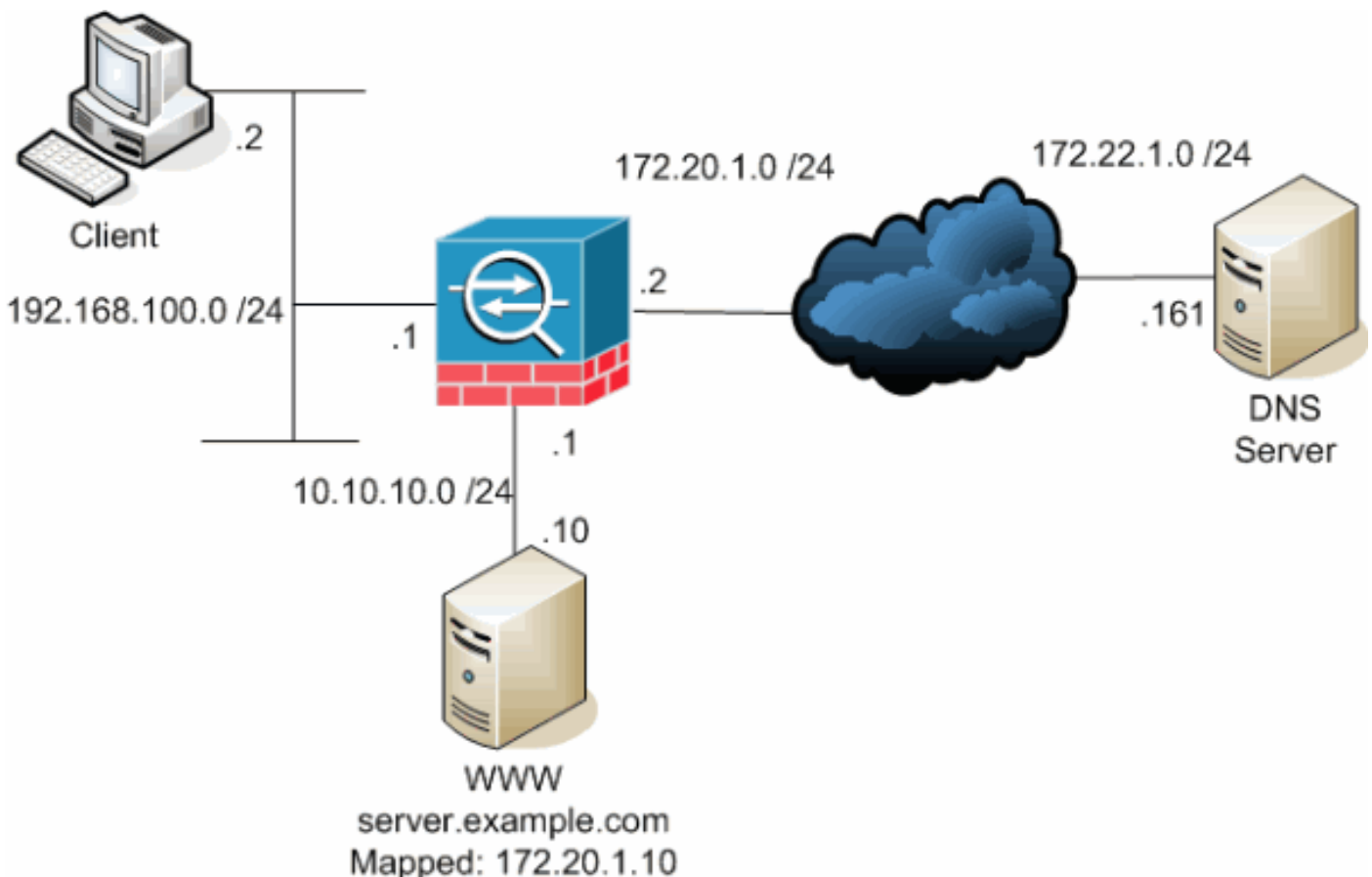
注：ASDM の設定はバージョン 7.x だけに適用できます。

背景説明

一般的なDNS交換では、クライアントはURLまたはホスト名をDNSサーバに送信して、そのホストのIPアドレスを決定します。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：内部、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server.example.com URLを使用して10.10.10.10のWWWサーバにアクセスしようとしています。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。DNSサーバは別のパブリックネットワークにあるため、WWWサーバのののプライベートIPアドレスはを知らません。代わりに、WWWサーバのマッピングされたアドレス172.20.1.10を認識します。したがって、DNSサーバにはserver.example.comから172.20.1.10への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、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、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.

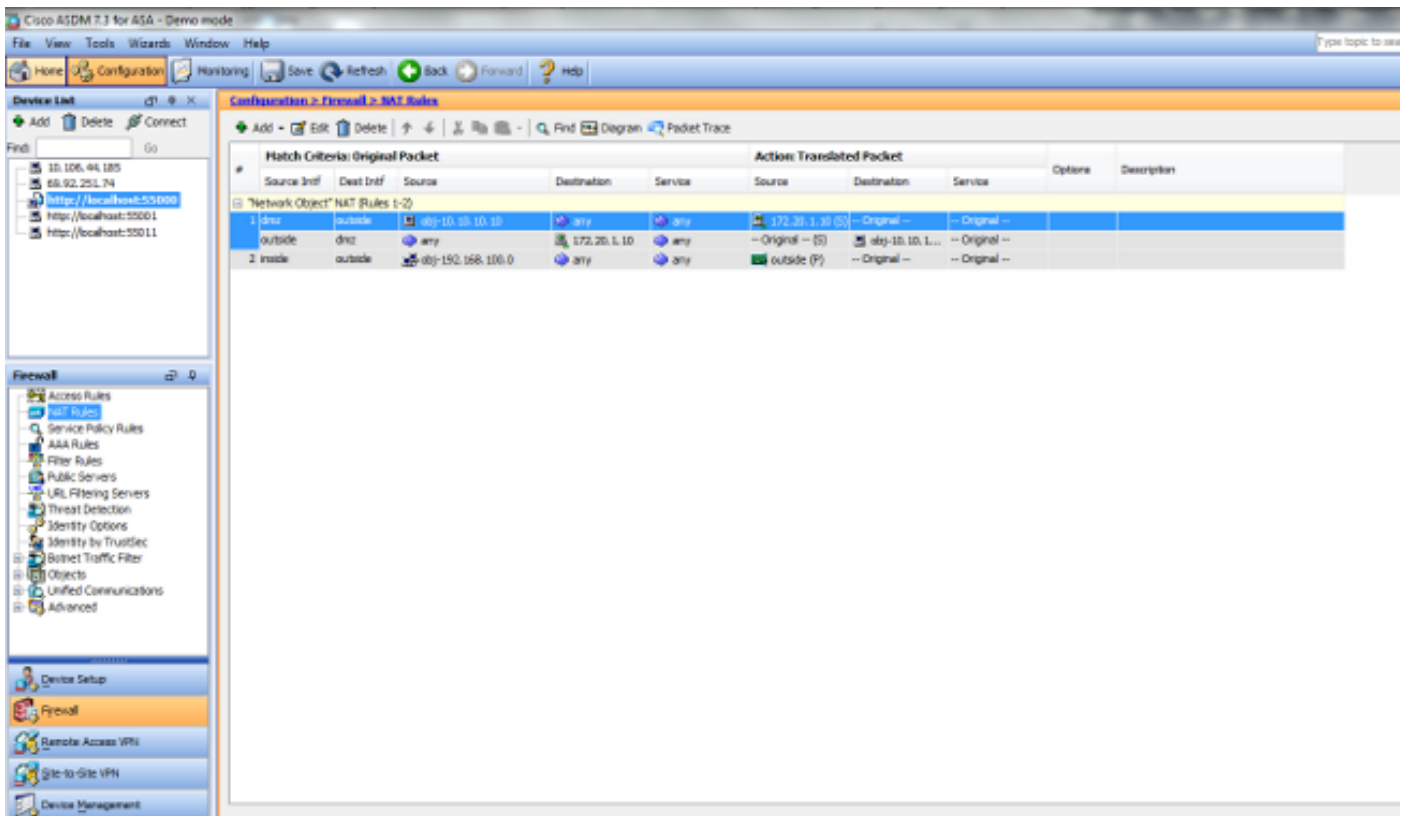
object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

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のWWWサーバにアクセスしようとしています。ASAは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。適切に設定すると、セキュリティアプライアンスはAレコードを変更して、「問題：Client Cannot Access WWW Server」セクションにアクセスして接続します。DNS Doctoringが有効な場合、セキュリティアプライアンスはAレコードを書き換え、クライアントを172.20.1.10ではなく10.10.10.10に転送します。DNS Doctoringは、スタティックNATステートメント（バージョン8.2以前）またはオブジェクト/自動NATステートメント（バージョン8.3以降）にdnsキーワードを追加すると有効になります。

バージョン8.2以前

これは、dnsキーワードと、バージョン8.2以前の3つのNATインターフェイスを使用してDNS Doctoringを実行するためのASAの最終的な設定です。

```
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. **Configuration > NAT Rules**の順に選択し、変更するObject/Autoルールを選択します。[Edit] をクリックします。
2. **[詳細]**をクリックします。

Edit Network Object

Name: obj-10.10.10.10

Type: Host

IP Version: IPv4 IPv6

IP Address: 10.10.10.10

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 172.20.1.10

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

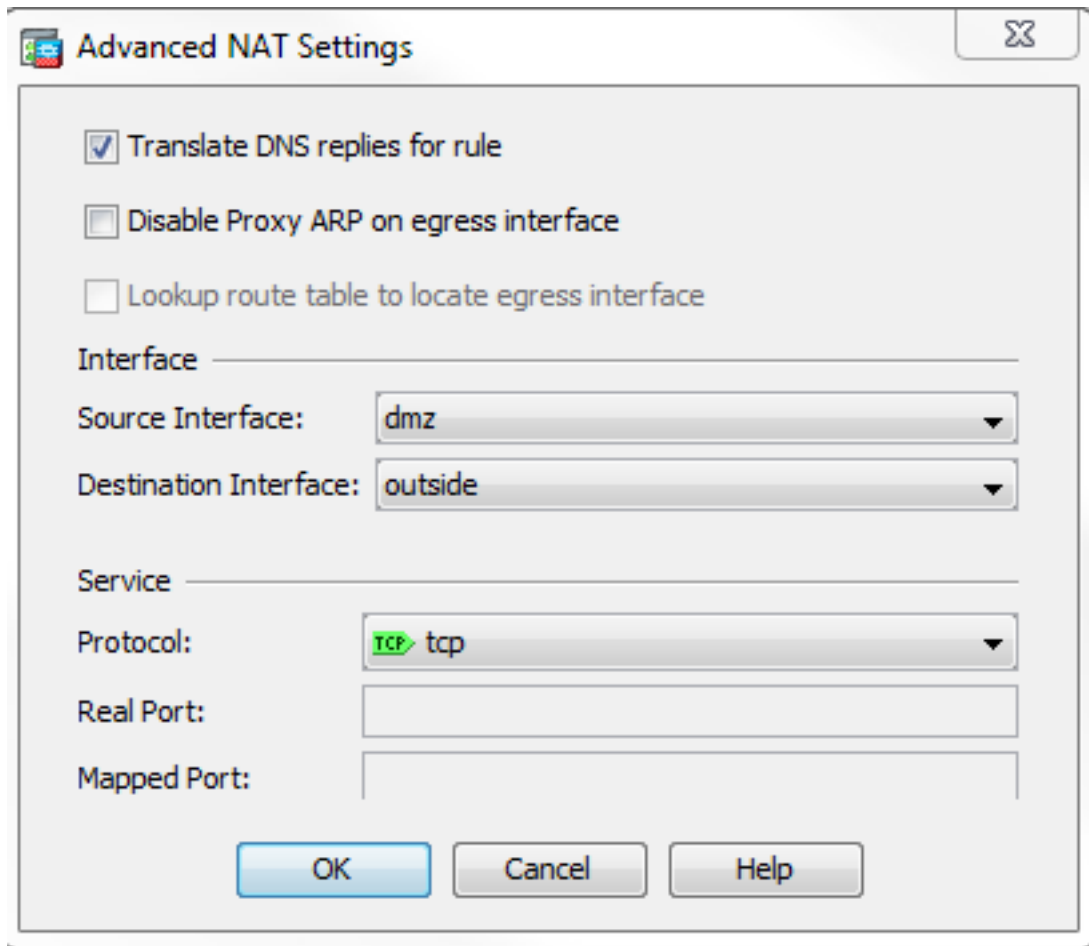
Fall through to interface PAT(dest intf): dmz

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

3. **[ルールに対するDNS応答の変換]**チェックボックスをオンにします。



4. [OK]をクリックして、[NAT Options]ウィンドウを閉じます。
5. [OK]をクリックして、[Edit Object/Auto NAT Rule]ウィンドウを閉じます。
6. [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。

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-shal
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。この状況で宛先NATを使用するには、内部のWWWサーバのパブリックアドレスとDMZの実アドレスの間にスタティックなオブジェクト/自動NAT変換が作成される必要があります。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。スタティックなオブジェクト/自動変換により、セキュリティアプライアンスは宛先アドレスを172.20.1.10から10.10.10.10に変換できます。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/2回のNAT文で実現される宛先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

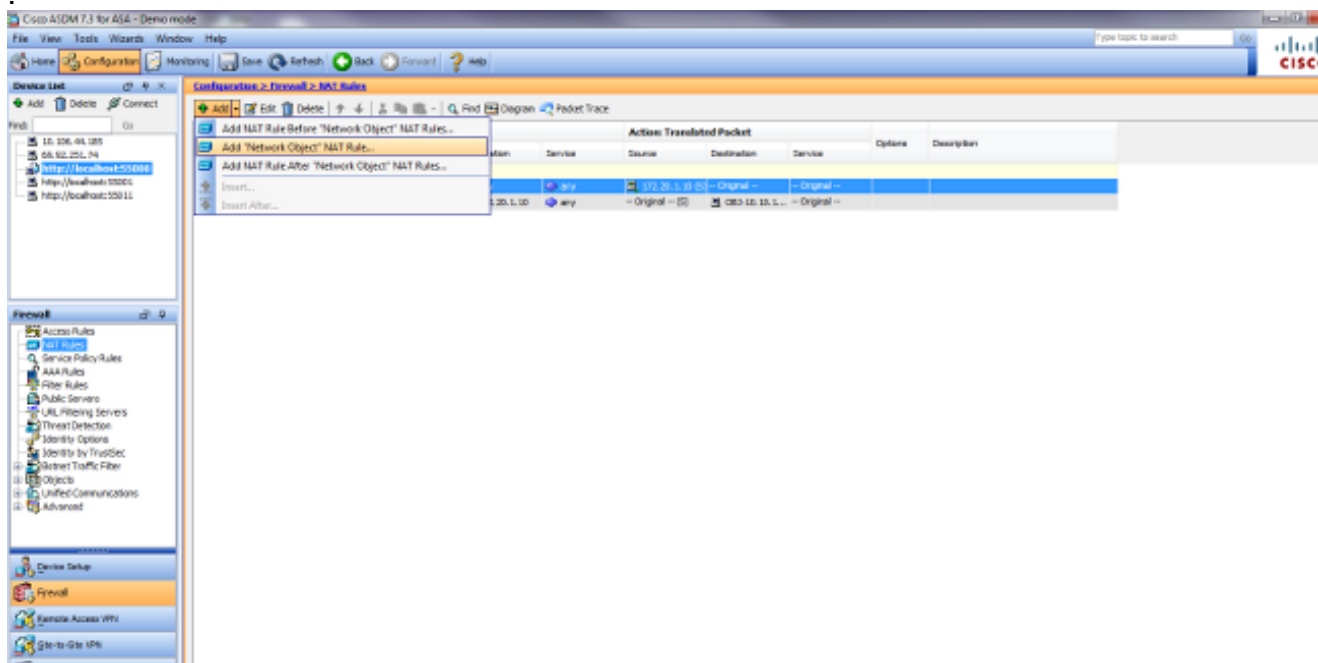
!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.

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. Configuration > NAT Rulesの順に選択し、Add > Add "Network Object" NAT Rule...を選択します。



2. 新しいスタティック変換の設定を入力します。[名前]フィールドにobj-10.10.10.10と入力します。[IP Address]フィールドに、WWWサーバのIPアドレスのアドレスを入力します。「タイプ」ドロップダウン・リストから「静的」を選択します。[Translated Addr]フィールドに、WWWサーバを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。[Advanced]をクリックします。

Add Network Object [Close]

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT [Up Arrow]

Add Automatic Address Translation Rules

Type:

Translated Addr: [...]

Use one-to-one address translation

PAT Pool Translated Address: [...]

Round Robin

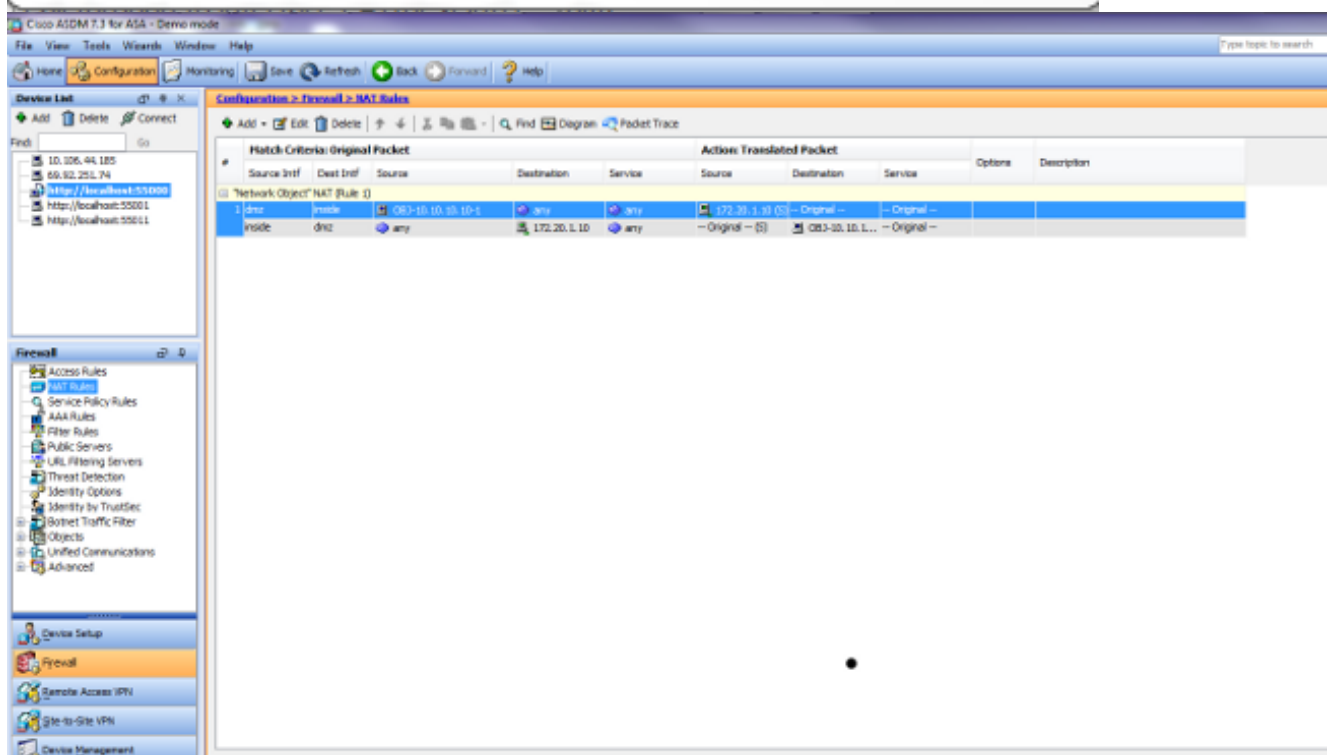
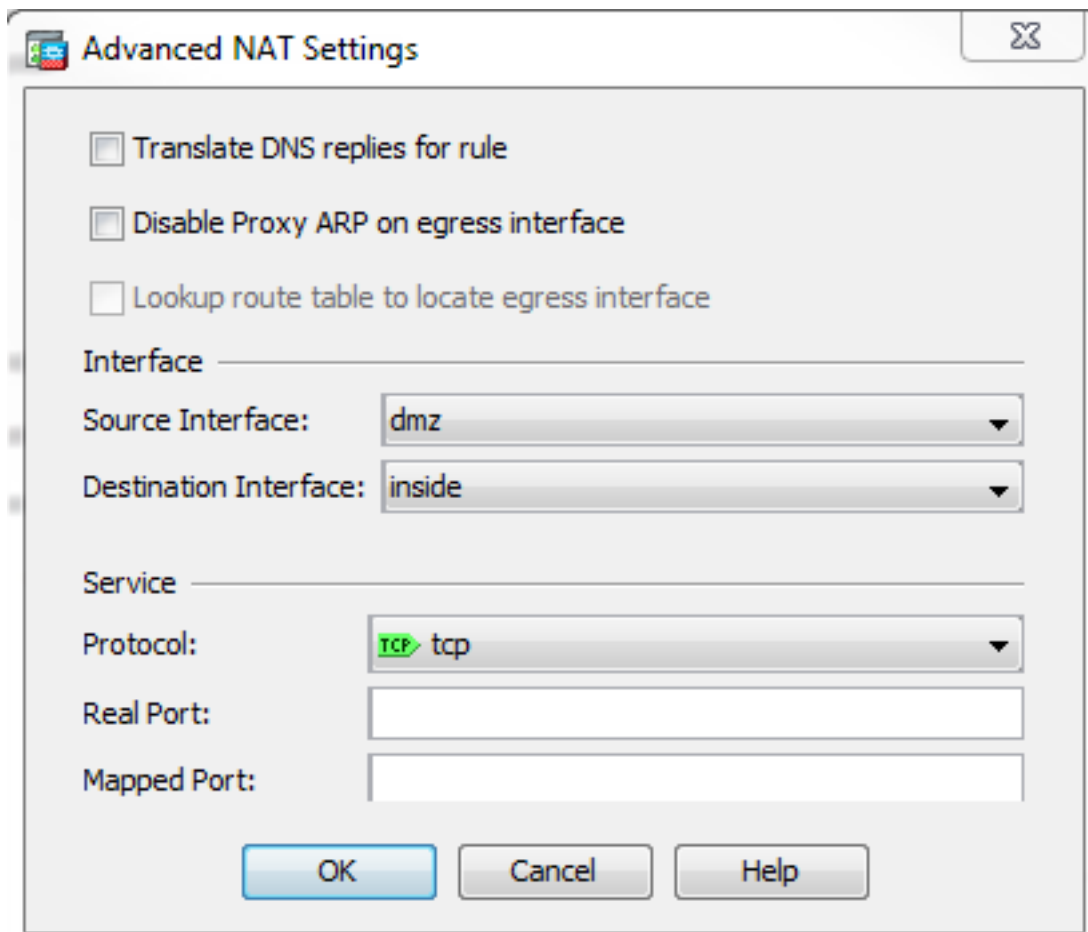
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

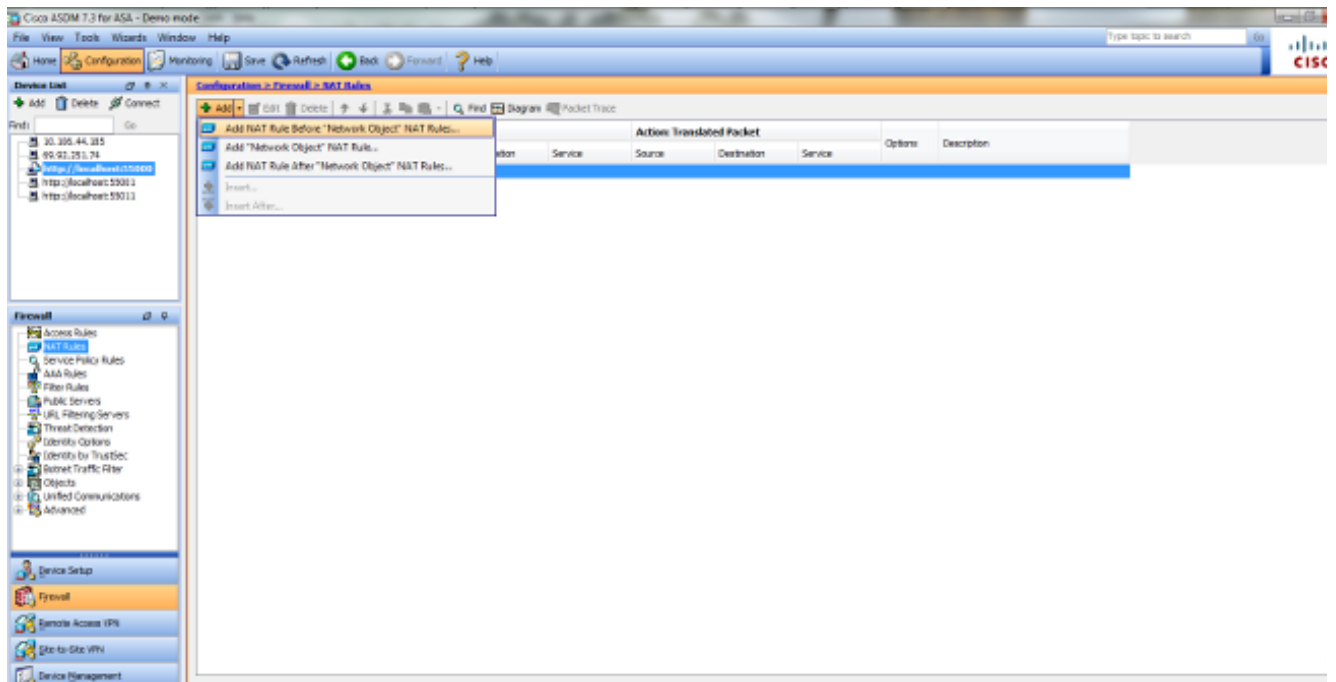
[Source Interface] ドロップダウンリストで、[dmz] を選択します。 [Destination Interface] ドロップダウンリストで、[inside] を選択します。 この例では、inside インターフェイス上のホストが、マップアドレス 172.20.1.10 を介して WWW サーバにアクセスできるように inside インターフェイスが選択されています。



[OK]をクリックして、[Add Object/Auto 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。

手動/2回のNATとASDMによる代替方式

1. Configuration > NAT Rulesの順に選択し、Add > Add Nat rule before "Network Object" NAT Rule...を選択します。



2. Manual/Twice Nat変換の設定を入力します。 [Source Interface]ドロップダウンリストで、 [inside]を選択します。 [Destination Interface]ドロップダウンリストで [dmz]を選択します。 [Source Address]フィールドに、 inside network object (obj-192.168.100.0)を入力します。 [Destination Address]フィールドに、 DMZサーバのIPオブジェクト(172.20.1.10)を変換します。 [Source NAT Type]ドロップダウンリストで、 [Dynamic PAT (Hide)]を選択します。 [Source Address [Action:[Translated Packet]セクション]フィールドにdmzと入力します。宛先住所[アクション : Translated Packet]セクションフィールドで、 DMZサーバの実IPオブジェクト(obj-10.10.10.10)を入力します。

Edit NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address:

Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

3. [OK]をクリックして、[Add Manual/ Twice NAT Rule]ウィンドウを閉じます。

4. [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。

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。

```
%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

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。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-shal
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спекションを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せん。

1. DNS 用のインспек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パラメータコンフィギュレーションモードに入り、インспекションエンジンのパラメータを指定します。

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

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

```
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спек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、ステップ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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の **show** コマンドをサポートします。OIT を使用して、**show** コマンドの出力の分析を表示します。

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。ACLは、キャプチャするトラフィックを指定する必要があります。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使用できる情報を示します。

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
```

xlate エントリをクリアしてから、このエラーを解決するために NAT ステートメントを削除して再適用します。

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 リファレンス](#)
- [セキュリティ製品に関する Field Notice](#)
- [Request for Comments \(RFC \)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)