配置医治为在ASA版本9.x的三个NAT接口的DNS

目录

简介

本文提供一配置示例执行医治在5500-X系列可适应安全工具的ASA的域名系统(DNS) (ASA)该用途反对/自动网络地址转换(NAT)语句。利用 DNS 修正，安全设备可以重写 DNS A 记录。

DNS 重写执行两项功能：

- 当 DNS 客户端位于专用接口上时，将 DNS 应答中的公共地址（可路由的或已映射的地址）转换为专用地址（实际地址）。
- 当 DNS 客户端位于公共接口上时，将专用地址转换为公共地址。

先决条件

要求

思科阐明，必须启用DNS检查为了执行医治在安全工具的DNS。默认情况下，DNS 检查处于启用状态。

如果 DNS 检查处于启用状态，安全设备将执行以下任务：

- 翻译DNS记录基于配置完成与使用对象/自动NAT命令(DNS重写)。转换仅适用于 DNS 应答中的 A 记录。所以反向查找，请求指示器(PTR)记录，没有影响的是受DNS重写的。在版本DNS PTR记录的ASA 9.0(1)及以后，转换为逆向DNS查找，当使用IPv4 NAT时， IPv6 NAT和NAT64中以DNS检查NAT规则。**注意**：DNS 重写与静态端口地址转换 (PAT) 不兼容，因为每个 A 记录有多条适用的 PAT 规则，并且要使用哪条 PAT 规则并非十分明确。
- 强制使用最大 DNS 消息长度（默认值是 512 个字节，最大长度是 65535 个字节）。重组如所需要进行为了验证数据包长度比配置的最大长度是较少。如果数据包超出最大长度，则会将其丢弃。**注意**：如果输入**Inspect dns**发出命令，不用最大长度选项，数据包大小没有被检查的DNS。
- 强制使用 255 个字节的域名长度和 63 个字节的标签长度。
- 验证当在 DNS 消息中遇到压缩指针时指针所指的域名的完整性。
- 检查是否存在压缩指针环路。

使用的组件

本文档中的信息根据ASA 5500-X系列安全工具，版本9.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置可能也与Cisco ASA 5500系列安全工具一起使用，版本8.4或以上。

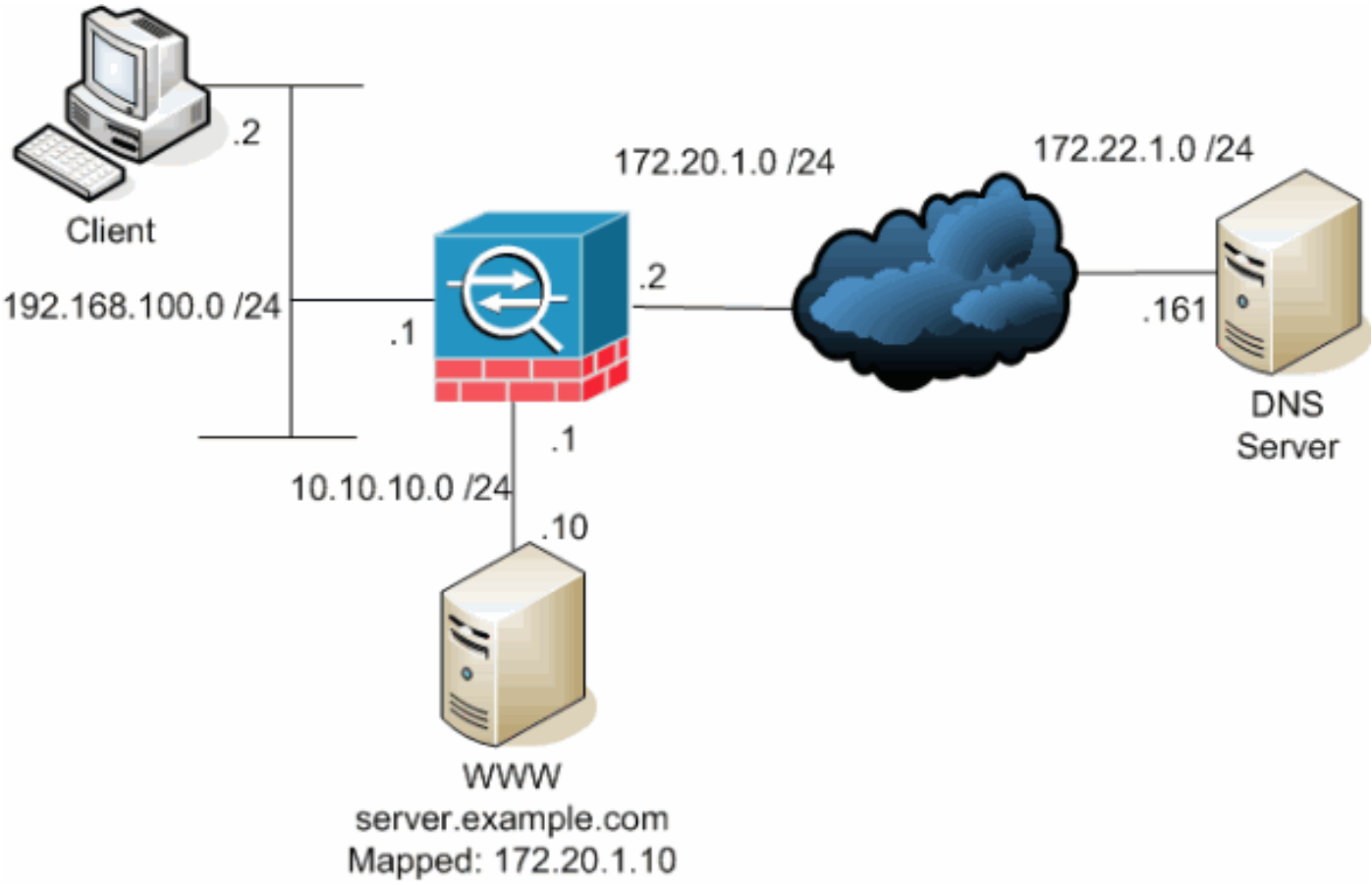
> **注意**：ASDM 配置仅适用于 7.x 版。

背景信息

在典型DNS中请交换，客户端发送URL或主机名到DNS服务器为了确定该主机的IP地址。DNS 服务器接收请求，查找该主机的“名称到 IP 地址”映射，然后将包含 IP 地址的 A 记录提供给客户端。虽然此过程在许多情况下都进行得很好，但也会发生一些问题。如果客户端和客户端尝试访问的主机均位于 NAT 后面的同一专用网络上，但客户端使用的 DNS 服务器位于另一个公共网络上，则会发生这些问题。

方案：三个NAT接口-里面，外部， DMZ

拓扑



此图说明了这种情况。在这种情况下， 192.168.100.2的客户端要使用**server.example.com** URL为了访问WWW服务器在10.10.10.10。客户端的 DNS 服务由地址为 172.22.1.161 的外部 DNS 服务器提供。由于 DNS 服务器位于另一个公共网络上，因此，它不知道 WWW 服务器的专用 IP 地址。然而，它知道 WWW 服务器的映射地址 172.20.1.10。因此，DNS 服务器包含 **server.example.com** 到 172.20.1.10 的“IP 地址到名称”映射。

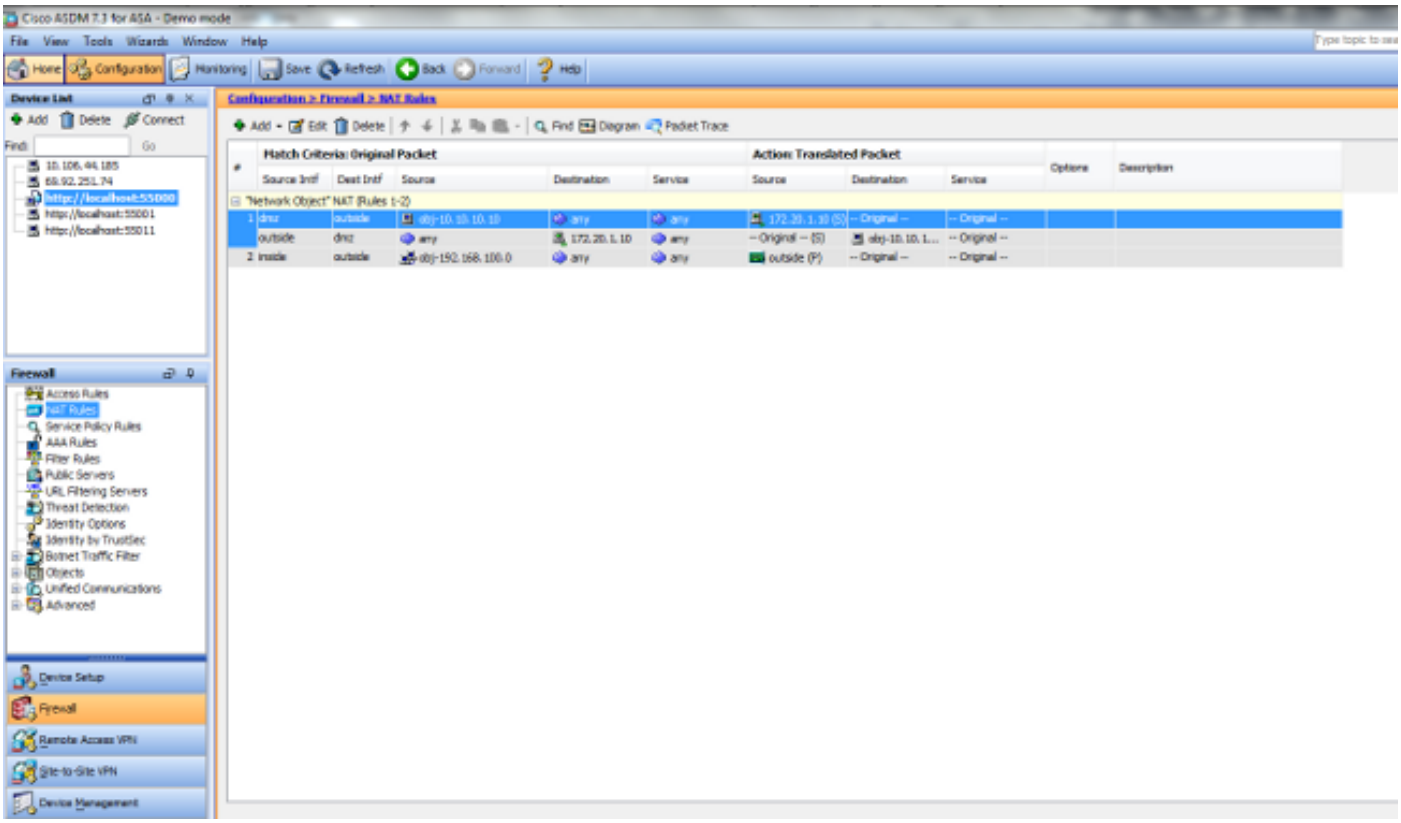
问题：客户端不能访问WWW服务器

如果在这种情况下未启用 DNS 修正或其他解决方案，则当客户端发送获取 **server.example.com** 的 IP 地址的 DNS 请求时将无法访问 WWW 服务器。这是因为，客户端接收的 A 记录包含 WWW 服务器的已映射公共地址 172.20.1.10。当客户端尝试访问此 IP 地址时，安全设备会丢弃数据包，因为它不允许在同一个接口上重定向数据包。当 DNS 修正处于禁用状态时配置的 NAT 部分如下所示：

```
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.
```

当 DNS 修正处于禁用状态时 ASDM 中的配置如下所示：



下面是当 DNS 修正处于禁用状态时事件的数据包捕获：

1. 客户端发送 DNS 查询。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 查询由 ASA 执行 PAT 并被转发。请注意，数据包的源地址已更改为 ASA 的外部接口。

```
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 服务器用 WWW 服务器的映射地址予以回复。

```
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 撤消 DNS 响应的目标地址的转换并将数据包转发到客户端。请注意，在未启用 DNS 修正的情况下，应答中的**地址**仍然是 WWW 服务器的映射地址。

```
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. 这时客户端设法访问WWW服务器在172.20.1.10。ASA 将为此通信创建连接项。然而，因为它不允许数据流从里向外流到 dmz，所以连接会超时。ASA 日志显示以下内容：`%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`**

解决方案：“dns”关键字

使用“dns”关键字进行 DNS 修正

使用 **dns** 关键字进行 DNS 修正，安全设备可以拦截和重写 DNS 服务器应答客户端的内容。当适当地配置，安全工具能修改A类记录为了在这种情况下允许客户端如“问题所述：客户端不能访问WWW服务器”部分连接。在这种情况下与启用的DNS医治，安全工具重写A类记录处理客户端到10.10.10.10而不是172.20.1.10。DNS医治启用，当您添加**dns**关键字到一个静态NAT语句(版本8.2和以下)时或反对/自动NAT语句(版本8.3和以上)。

版本8.2和以下

这是执行DNS的ASA的最终配置医治与**dns**关键字和三个NAT接口版本8.2和以下的。

```
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
```

版本8.3和以上

```
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.
```

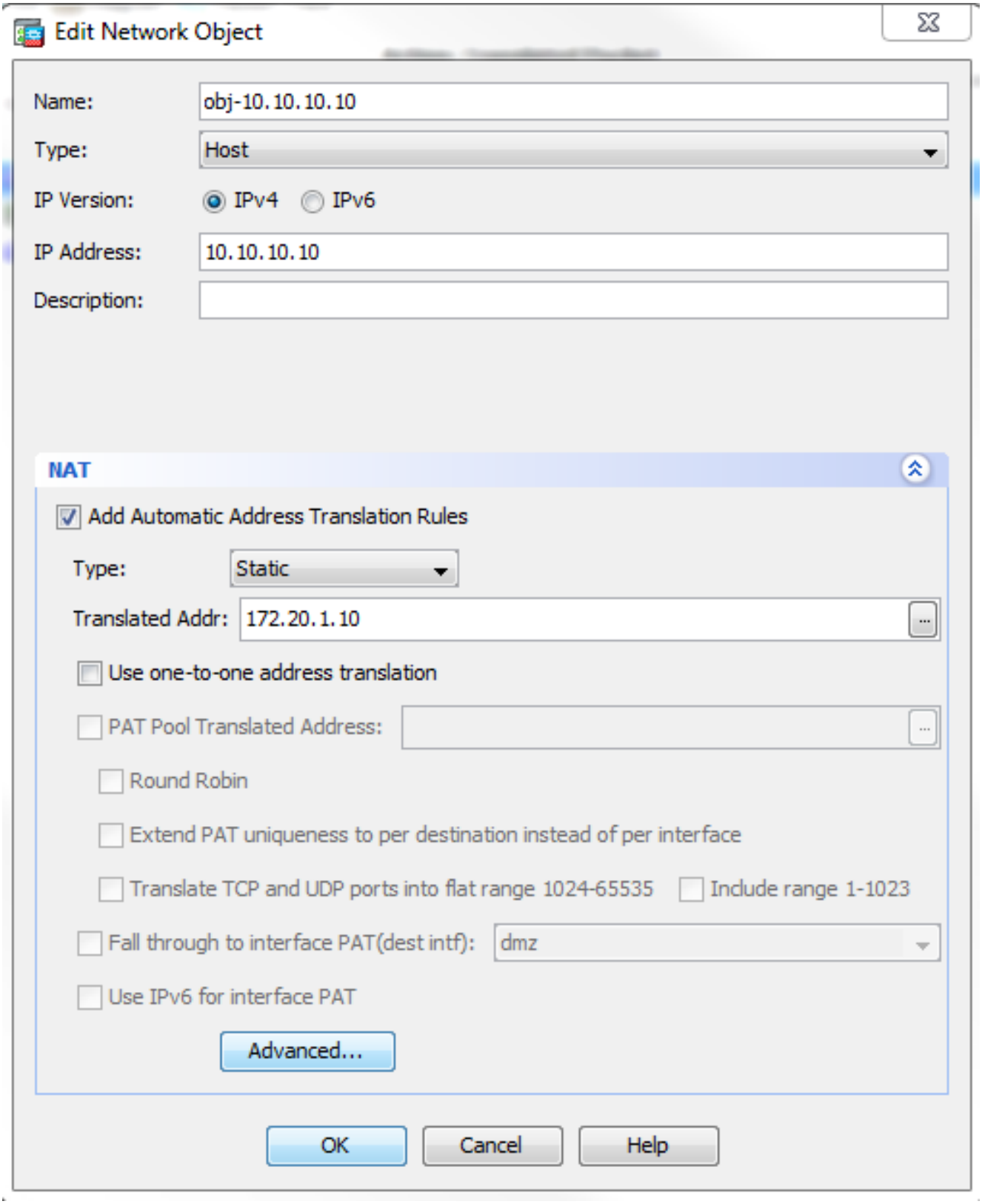
ASDM 配置

要在 ASDM 中配置 DNS 修正，请完成以下步骤：

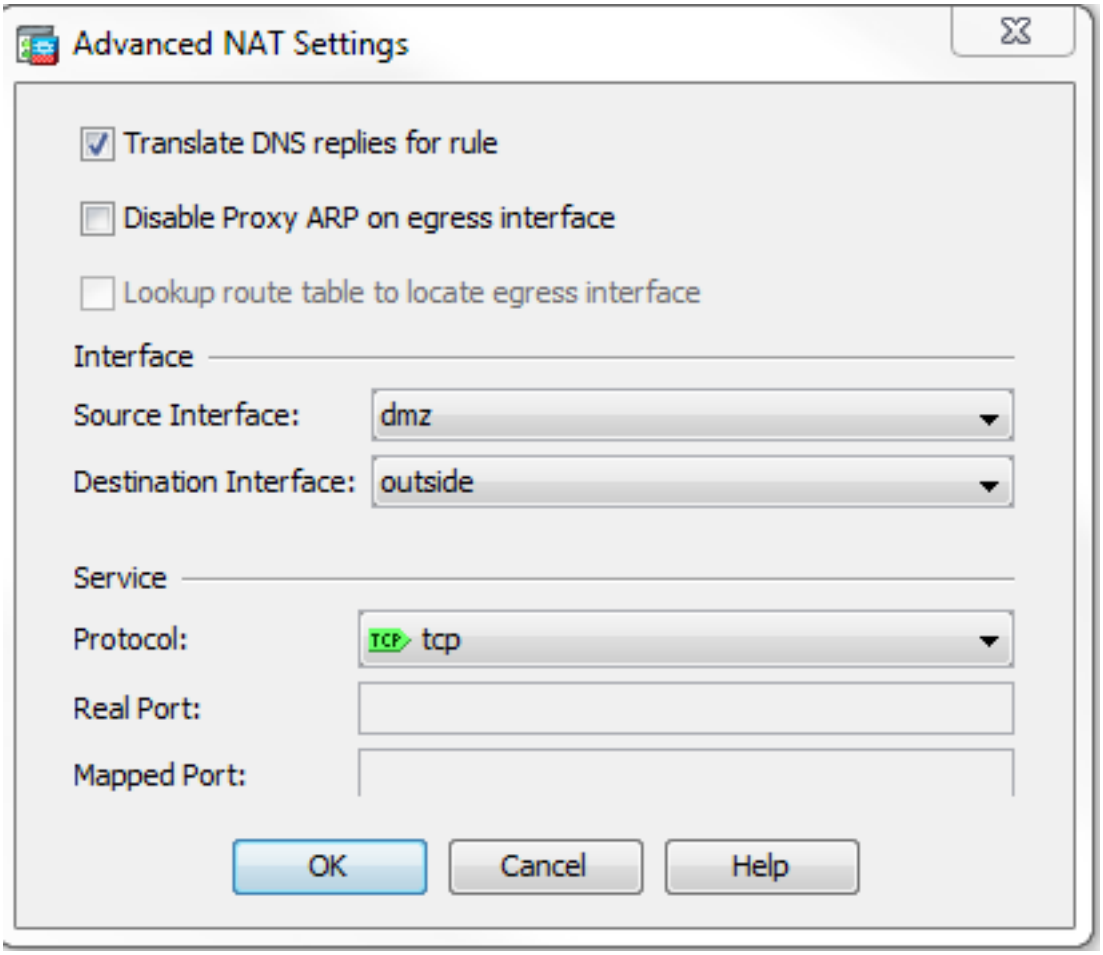
1. 选择**Configuration> NAT规则**并且选择对象/自动规则被修改。单击 **Edit**。

2. 点击**先进**

...



3. 检查**翻译DNS为规则**复选框**回复**。



4. 点击OK键为了留下NAT选项窗口。
5. 点击OK键为了留下编辑对象/自动NAT规则窗口。
6. 单击**应用**为了发送您的配置到安全工具。

验证

下面列出了当 DNS 修正处于启用状态时事件的数据包捕获：

1. 客户端发送 DNS 查询。

```
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 查询由 ASA 执行 PAT 并被转发。请注意，数据包的源地址已更改为 ASA 的外部接口。

```
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 服务器用 WWW 服务器的映射地址予以回复。

```
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 撤消 DNS 响应的目标地址的转换并将数据包转发到客户端。请注意，在 DNS 修正处于启用状态时，会将应答中的**地址**重写为 WWW 服务器的实际地址。

```
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. 此时，客户端设法访问 10.10.10.10 处的 WWW 服务器。连接成功。

使用“dns”关键字进行的最终配置

这是要使用 **dns** 关键字和三个 NAT 接口执行 DNS 修正的 ASA 的最终配置。

```
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
```

备用解决方案：目标 NAT

目标 NAT 可以提供 DNS 修正的备用方案。在这种情况下使用目的地NAT要求静态对象/自动NAT转换创建在里面的WWW服务器在DMZ的公共地址和实际地址之间。目标 NAT 不会更改从 DNS 服务器返回到客户端的 DNS A 记录的内容。相反，当您在诸如本文档中讨论的场景下使用目标 NAT 时，客户端可以使用由 DNS 服务器返回的公用 IP 地址 172.20.1.10 来连接到 WWW 服务器。静态对象/自动转换允许安全工具转换从172.20.1.10的目的地址到10.10.10.10。下面列出了当使用目标 NAT 时配置的相关部分：

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

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

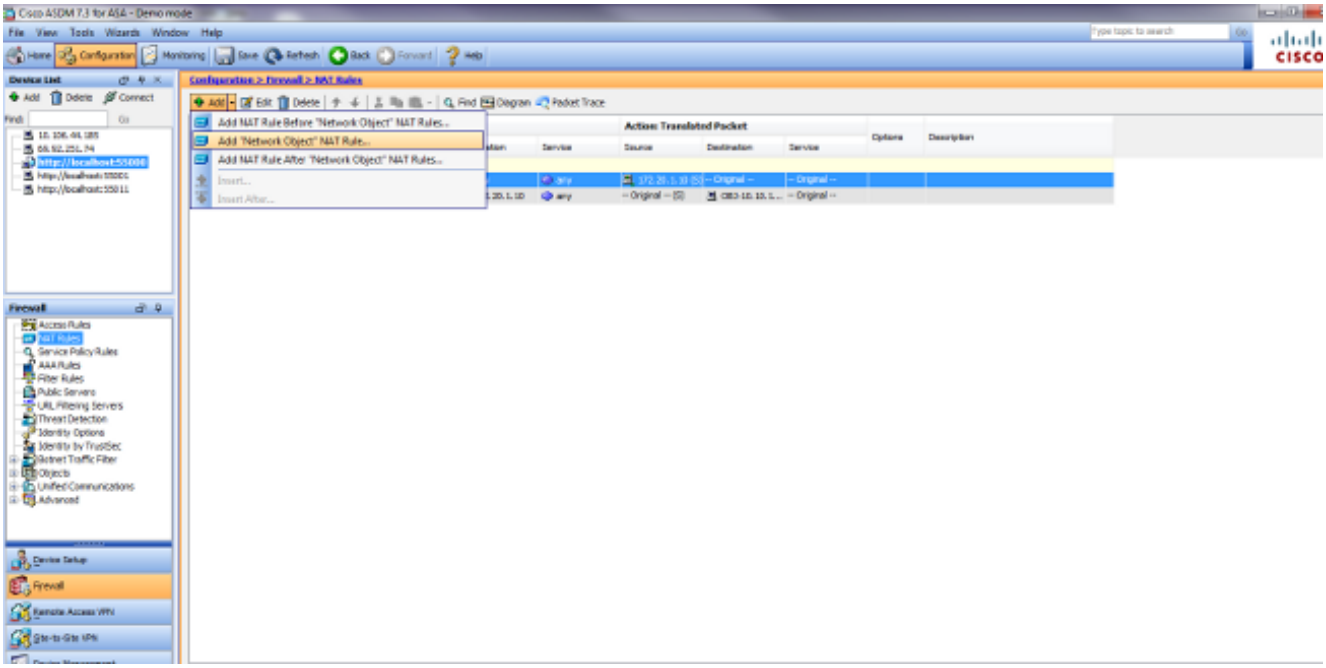
```
!--- Output suppressed.

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
```

用指南/两次NAT语句完成的目的地NAT

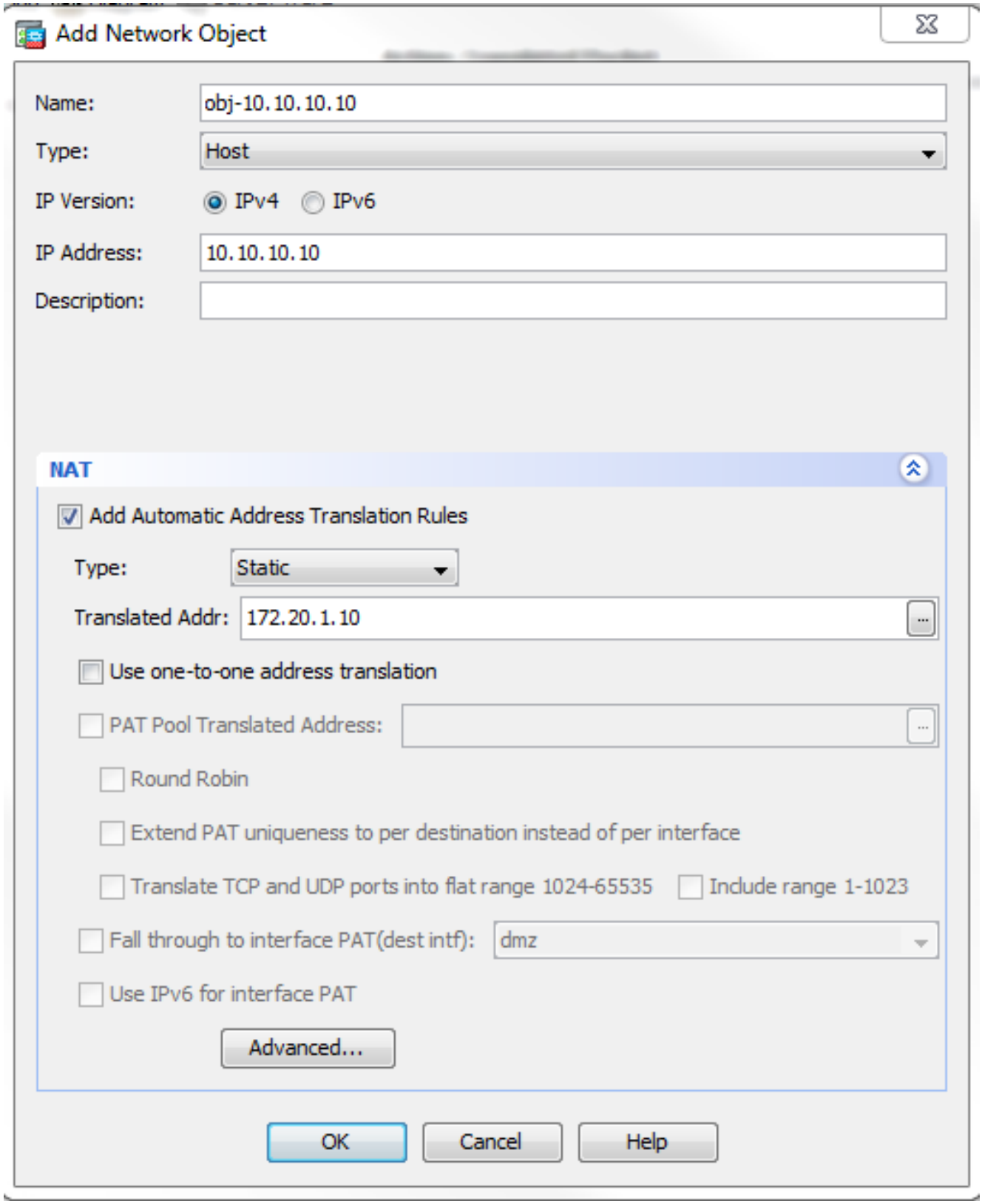
```
ASA Version 9.x
!
hostname ciscoasa

!--- 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.
```

要在 ASDM 中配置目标 NAT，请完成以下步骤：

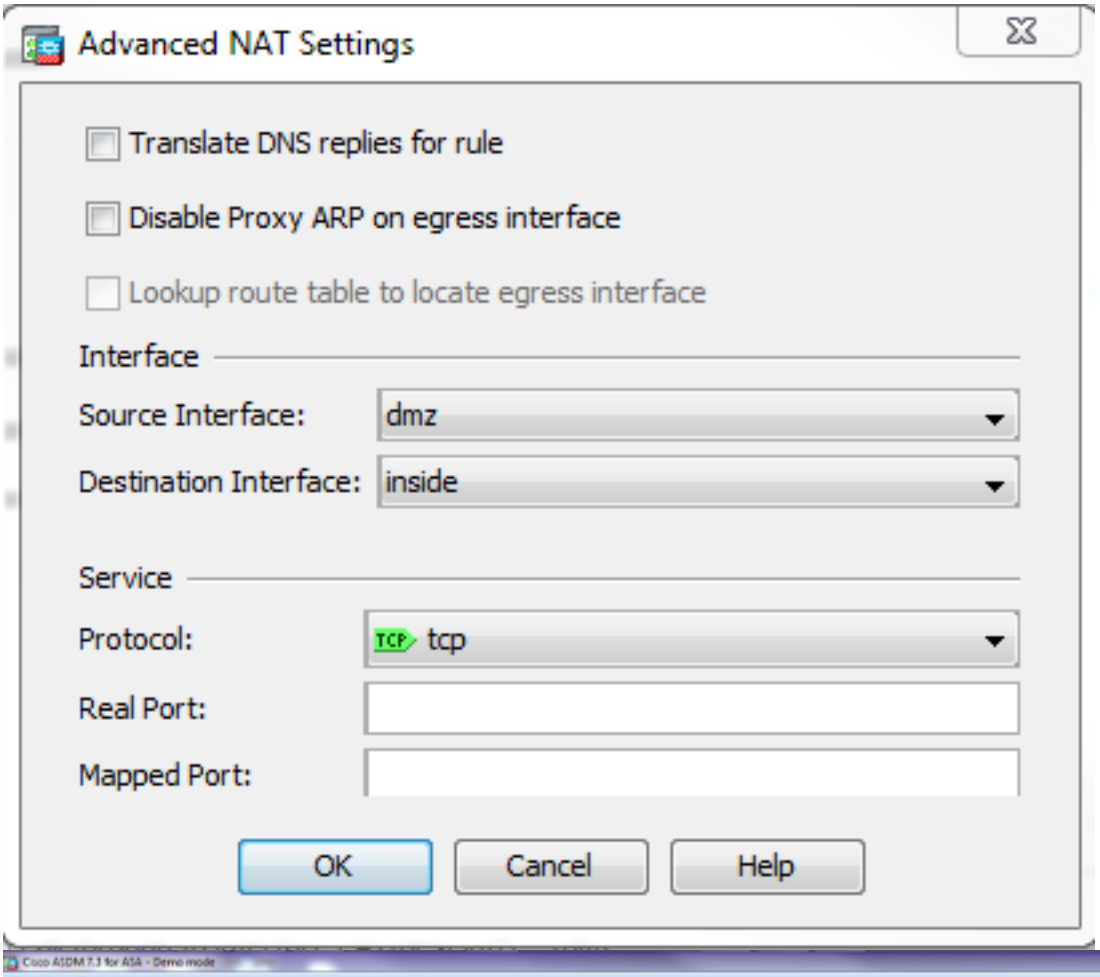
1. 选择**Configuration> NAT规则**并且选择**Add>增加“网络对象” NAT规则**
   ....

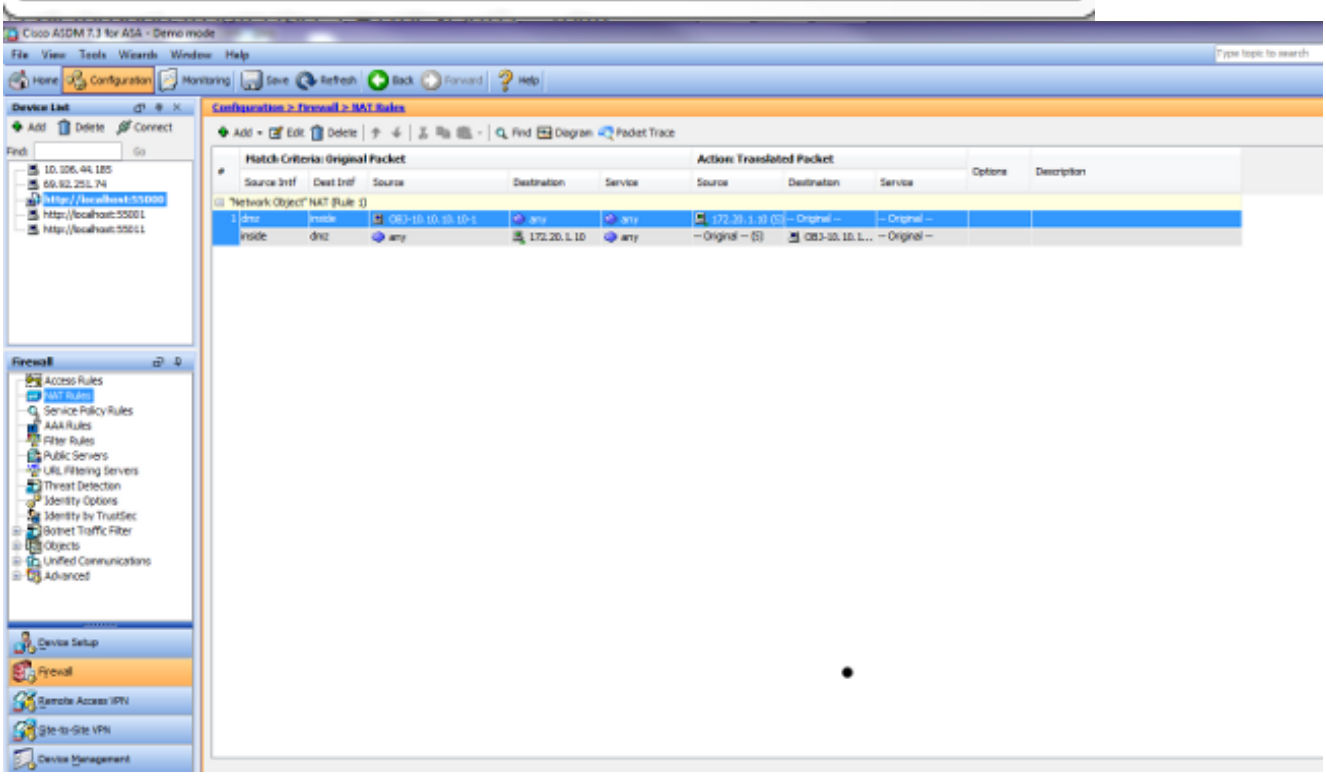


2. 填写新静态转换的配置。 在Name字段，请输入**obj-10.10.10.10**。在IP地址字段，请输入WWW服务器IP地址的地址。从类型下拉列表，请选择**静态**。在翻译的地址字段，请进入地址和接口您要映射WWW服务器。单击 **Advanced**。



在源接口下拉列表中，请选择**dmz**。在目的地接口下拉列表中，请选择**里面**。在这种情况下，选择内部接口以允许内部接口上的主机通过映射的地址 172.20.1.10 访问 WWW 服务器。

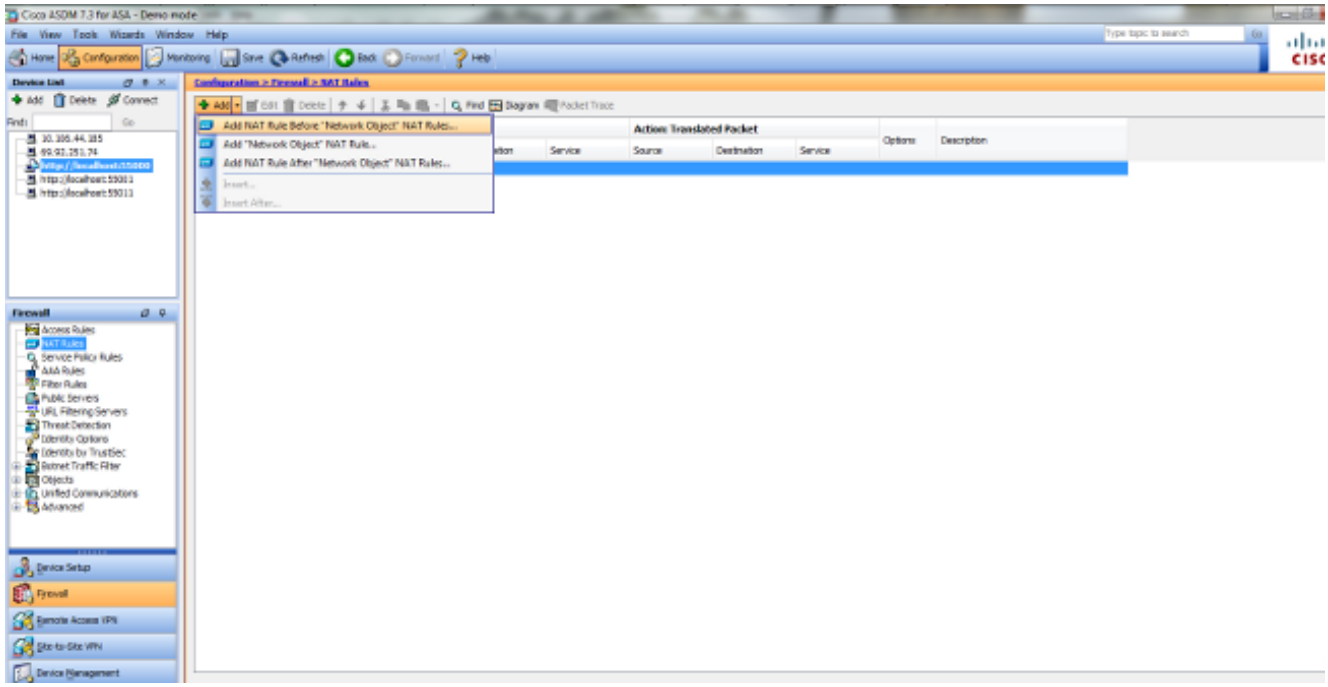




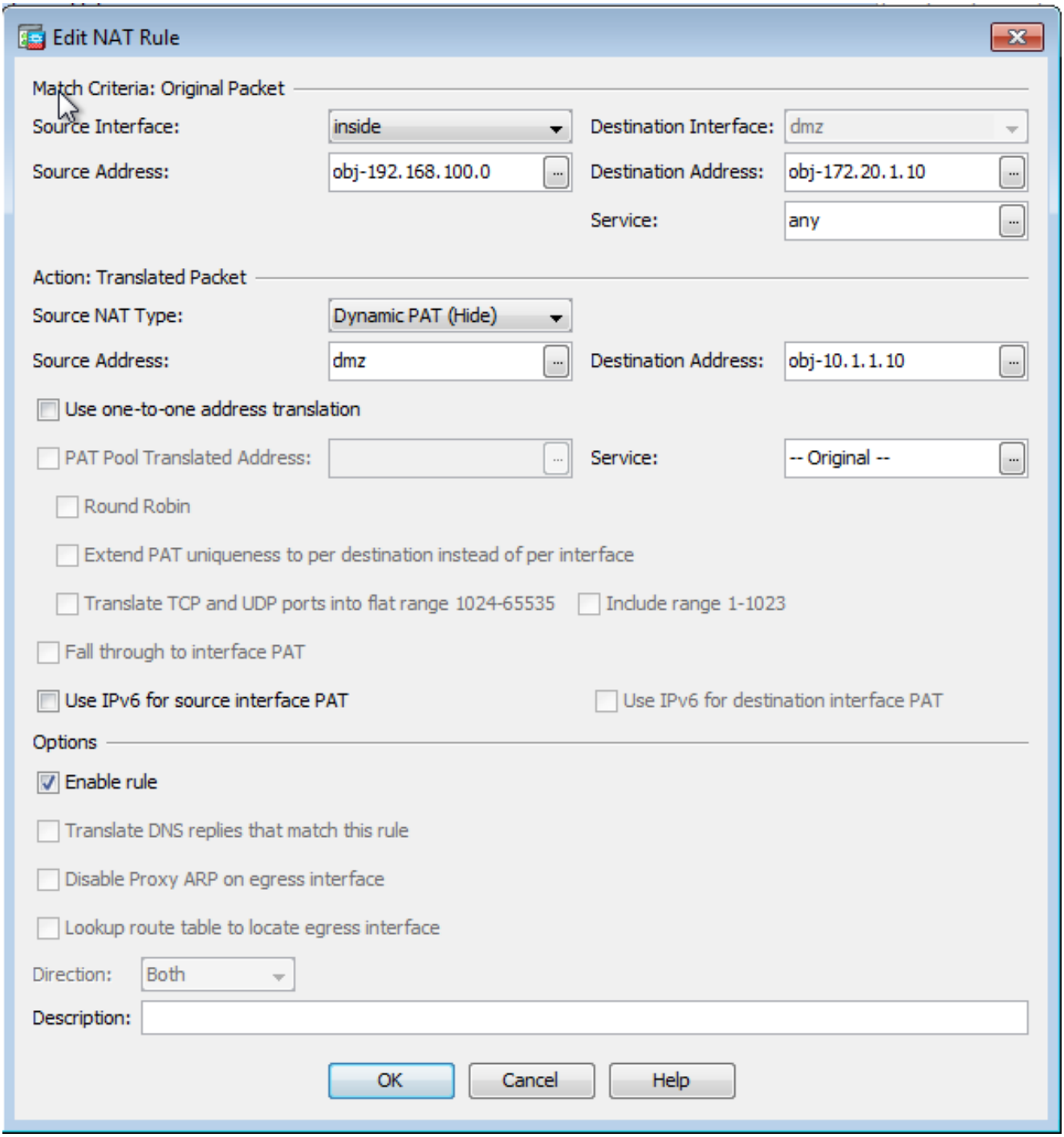
点击OK键为了留下添加对象/自动NAT规则窗口。单击**应用**为了发送配置到安全工具。

与指南/两次NAT和ASDM的替代方法

1. 请选择**Configuration> NAT规则**并且选择**Add>增加nat规则，在“网络对象” NAT规则....前**



2. 填写手工/两次nat转换的配置。 在源接口下拉列表中，请选择**里面**。在目的地接口下拉列表中，请选择**dmz**。在源地址域，请输入网络内部对象(obj-192.168.100.0)。在目的地址字段，请输入翻译的DMZ服务器IP对象(172.20.1.10)。在来源NAT类型下拉列表中，请选择**动态PAT(隐藏)**。在源地址[操作：翻译的数据包部分]字段，输入**dmz**。在目的地址[操作：翻译的数据包部分]字段，输入DMZ服务器实时IP对象(obj-10.10.10.10)。



3. 点击OK键为了留给添加手工/两次NAT规则窗口。
4. 单击**应用**为了发送配置到安全工具。

下面列出了当配置目标 NAT 时发生的事件顺序。假设客户端已经查询了 DNS 服务器并且收到了 WWW 服务器地址的 **172.20.1.10** 应答：

1. 客户端尝试联系地址为 172.20.1.10 的 WWW 服务器。`%ASA-7-609001: Built local-host inside:192.168.100.2`
2. 安全设备查看请求并认为 WWW 服务器位于 10.10.10.10 处。`%ASA-7-609001: Built local-host dmz:10.10.10.10`
3. 安全设备在客户端和 WWW 服务器之间创建 TCP 连接。请注意括号内每台主机的映射地址。
   `%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. 安全设备上的 **show xlate** 命令可验证客户端数据流是否通过安全设备进行转换。在这种情况下，使用第一种静态转换。`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. 安全设备上的 **show conn** 命令验证是否已通过安全设备成功地在客户端和 WWW 服务器之间建立了连接。请注意括号内 WWW 服务器的实际地址。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
```

使用目标 NAT 的最终配置

这是要使用目标 NAT 和三个 NAT 接口执行 DNS 修正的 ASA 的最终配置。

```
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
```

配置

要启用 DNS 检查（如果以前禁用），请完成以下步骤。在本示例中，将 DNS 检查添加到默认全局检查策略中，该策略由 service-policy 命令全局应用，就好像 ASA 以默认配置开始一样。

1. 为 DNS 创建检查策略映射。ciscoasa(config)#**policy-map type inspect dns MY_DNS_INSPECT_MAP**
2. 从policy-map配置模式，请输入参数配置模式为了指定检测引擎的参数。ciscoasa(config-pmap)#**parameters**
3. 在策略映射参数配置模式，请指定DNS消息的最大消息长度能是512。ciscoasa(config-pmap-p)#**message-length maximum 512**
4. 退出策略映射参数配置模式和策略映射配置模式。ciscoasa(config-pmap-p)#**exit**
   ciscoasa(config-pmap)#**exit**
5. 请确认是否已根据需要创建了检查策略映射。ciscoasa(config)#**show run policy-map type inspect dns**
   ```
   !
   policy-map type inspect dns MY_DNS_INSPECT_MAP
   parameters
   message-length maximum 512
   !
   ```
6. 进入 global_policy 的策略映射配置模式。ciscoasa(config)#**policy-map global_policy**
   ciscoasa(config-pmap)#
7. 在策略映射配置模式下，指定默认层 3/4 类映射 inspection_default。ciscoasa(config-pmap)#**class inspection_default**
   ciscoasa(config-pmap-c)#
8. 在策略映射等级配置模式，请使用创建的检查策略映射在步骤1-3为了指定应该检查DNS。
   ciscoasa(config-pmap-c)#**inspect dns MY_DNS_INSPECT_MAP**
9. 退出策略映射类配置模式和策略映射配置模式。ciscoasa(config-pmap-c)#**exit**
   ciscoasa(config-pmap)#**exit**
10. 验证是否已根据需要配置 global_policy 策略映射。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. 验证服务策略是否已全局应用 global_policy。`ciscoasa(config)#show run service-policy`
```
service-policy global_policy global
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

捕获 DNS 数据流

其中一个验证安全设备是否可正确重写 DNS 记录的方法是捕获相关数据包，如上一示例中所述。要在 ASA 上捕获数据流，请完成以下步骤：

1. 为您要创建的每个捕获实例创建一个访问列表。ACL 应该指定您希望捕获的数据流。在本示例中，已创建两个 ACL。 外部接口上数据流的 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.
```

内部接口上数据流的 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. 创建捕获实例：`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. 查看捕获。在传递了一些 DNS 数据流之后，捕获示例如下所示：
```
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. （可选）以 pcap 格式将捕获复制到 TFTP 服务器以在另一个应用程序中执行分析。可解析 pcap 格式的应用程序可以在 DNS A 记录中显示其他详细信息，如名称和 IP 地址。
```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

没有执行 DNS 重写

确保在安全设备上配置了 DNS 检查。

转换创建失败

如果无法在客户端和 WWW 服务器之间创建连接，则可能是由于 NAT 误配置所致。检查安全设备日志，查找指出协议无法通过安全设备创建转换的消息。如果出现这类消息，请验证是否已经为所需的数据流配置了 NAT 以及是否不存在错误的地址。

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

清除xlate条目，然后删除并且重新应用NAT语句为了解决此错误。

相关信息

- 思科ASA 5500-x配置指南
- Cisco ASA 5500-x系列命令参考
- 安全产品售后通知
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems