# PIX/ASA：使用静态命令和两个NAT接口执行医治的DNS配置示例

## 目录



## 简介

本文档针对以下操作提供了配置示例：使用静态网络地址转换 (NAT) 语句在 ASA 5500 系列自适应安全设备或 PIX 500 系列安全设备上执行域名系统 (DNS) 修正。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。

**注意：** 本文档中的配置包含两个 NAT 接口；内部和外部。有关使用 static 命令和三个 NAT 接口（内部、外部和 dmz）进行 DNS 修正的示例，请参阅 PIX/ASA：使用 static 命令和三个 NAT 接口配置示例执行 DNS 修正。

有关如何在安全设备上使用 NAT 的详细信息，请参阅 PIX/ASA 7.x NAT 和 PAT 语句以及在 PIX 上使用 nat、global、static、conduit 和 access-list 命令及端口重定向（转发）。

# 先决条件

## 要求

必须启用 DNS 检查，才可以在安全设备上执行 DNS 修正。默认情况下，DNS 检查处于启用状态。如果该检查处于禁用状态，请参阅本文档后面的配置 DNS 检查部分以将其重新启用。如果 DNS 检查处于启用状态，安全设备将执行以下任务：

- 根据使用 **static** 和 nat 命令（DNS 重写）完成的配置转换 DNS 记录。转换仅适用于 DNS 应答中的 A 记录。因此，DNS 重写不会影响用于请求 PTR 记录的反向查找。**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）。根据需要执行重组，以验证数据包长度是否短于所配置的最大长度。如果数据包超出最大长度，则会将其丢弃。**注意：** 如果在不使用最大长度选项的情况下发出 **inspect dns** 命令，则不会检查 DNS 数据包的大小。
- 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

本文档中的信息基于 ASA 5500 系列安全设备 7.2(1) 版。

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

此配置还可用于 Cisco PIX 500 系列安全设备 6.2 版或更高版本。

**注意：** Cisco 自适应安全设备管理器 (ASDM) 配置仅适用于 7.x 版。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

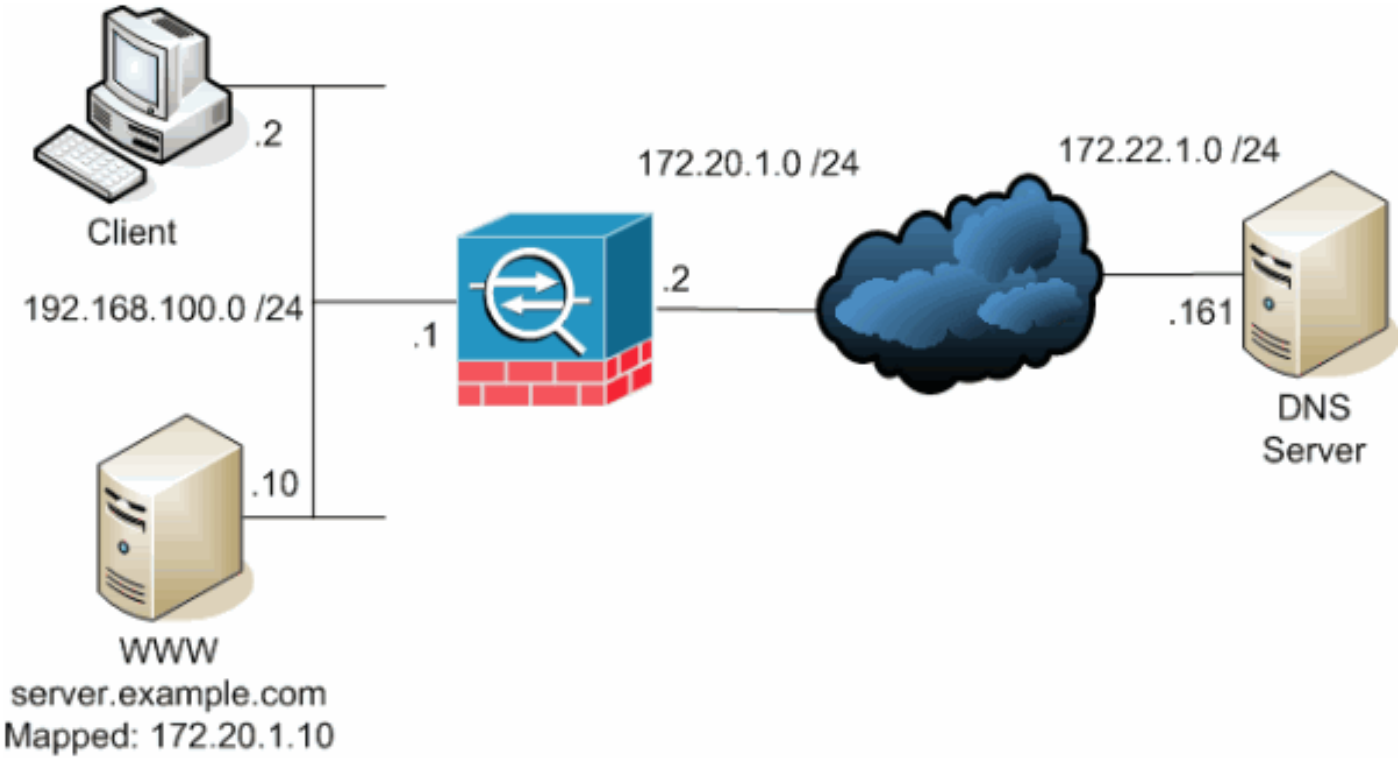
# 背景信息

在典型的 DNS 交换中，客户端将 URL 或主机名发送到 DNS 服务器，以确定该主机的 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：两个 NAT 接口（内部、外部）

## 拓扑

在此场景中，客户端和客户端尝试访问的 WWW 服务器均位于 ASA 的内部接口上。将动态 PAT 配置为允许客户端对 Internet 进行访问。将带有 access-list 的静态 NAT 配置为不但允许 Internet 主机访问 WWW 服务器，而且允许 WWW 服务器访问 Internet。



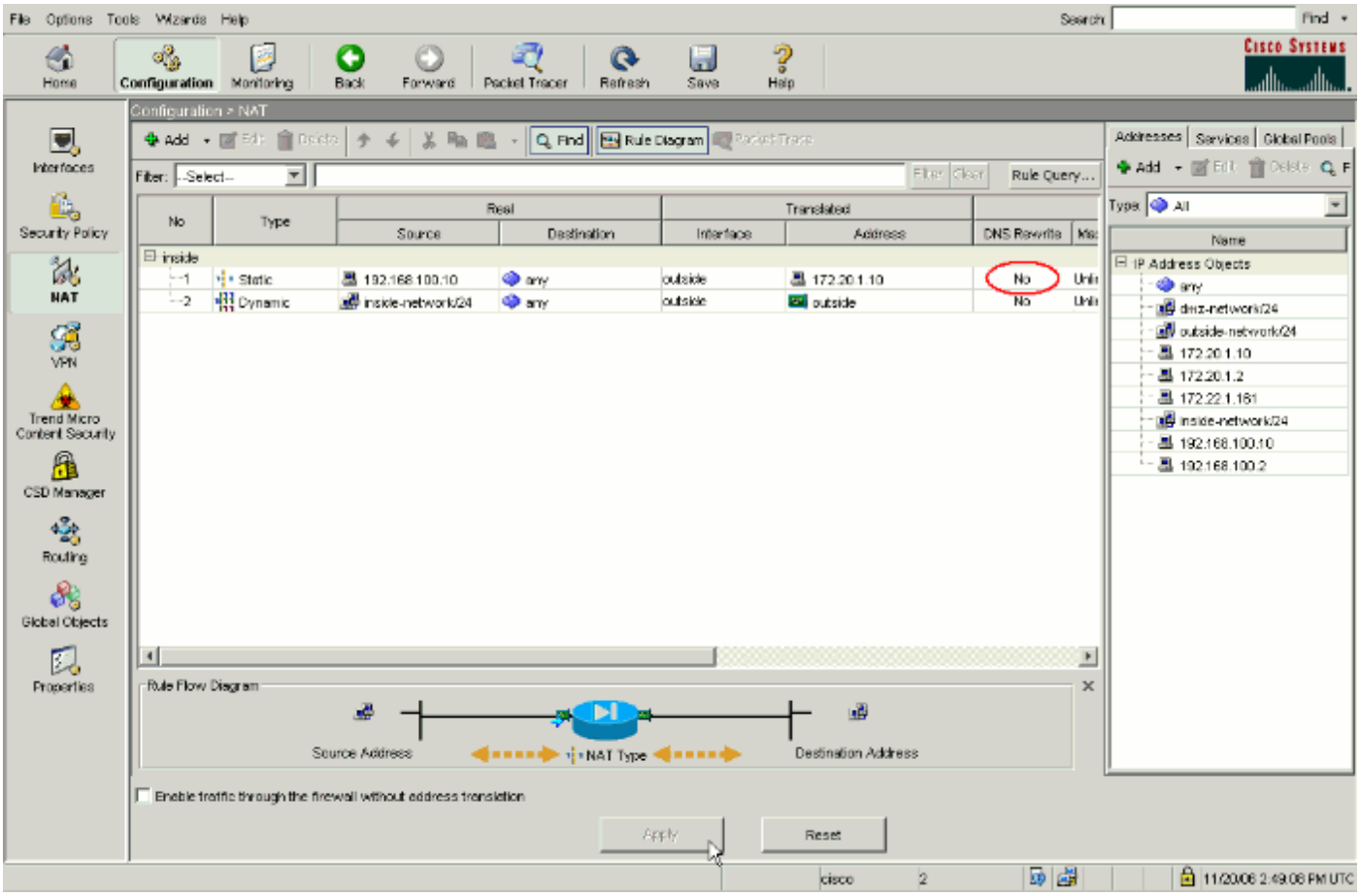

此图说明了这种情况。在这种情况下，地址为 192.168.100.2 的客户端希望使用 **server.example.com** URL 来访问地址为 192.168.100.10 的 WWW 服务器。客户端的 DNS 服务由地址为 172.22.1.161 的外部 DNS 服务器提供。由于 DNS 服务器位于另一个公共网络上，因此，它不知道 WWW 服务器的专用 IP 地址。然而，它知道 WWW 服务器的映射地址 172.20.1.10。因此，DNS 服务器包含 **server.example.com** 到 172.20.1.10 的“IP 地址到名称”映射。

## 问题：客户端无法访问 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 服务器的映射的公共地址：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：

```
ciscoasa(config)#show running-config : Saved : ASA Version 7.2(1) ! hostname ciscoasa !---
Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 access-group OUTSIDE
in interface outside !--- Output suppressed.
```

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. 此时，客户端尝试访问地址为 172.20.1.10 的 WWW 服务器。ASA 将为此通信创建连接项。然而，因为它不允许数据流从内部流到外部再流回内部，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

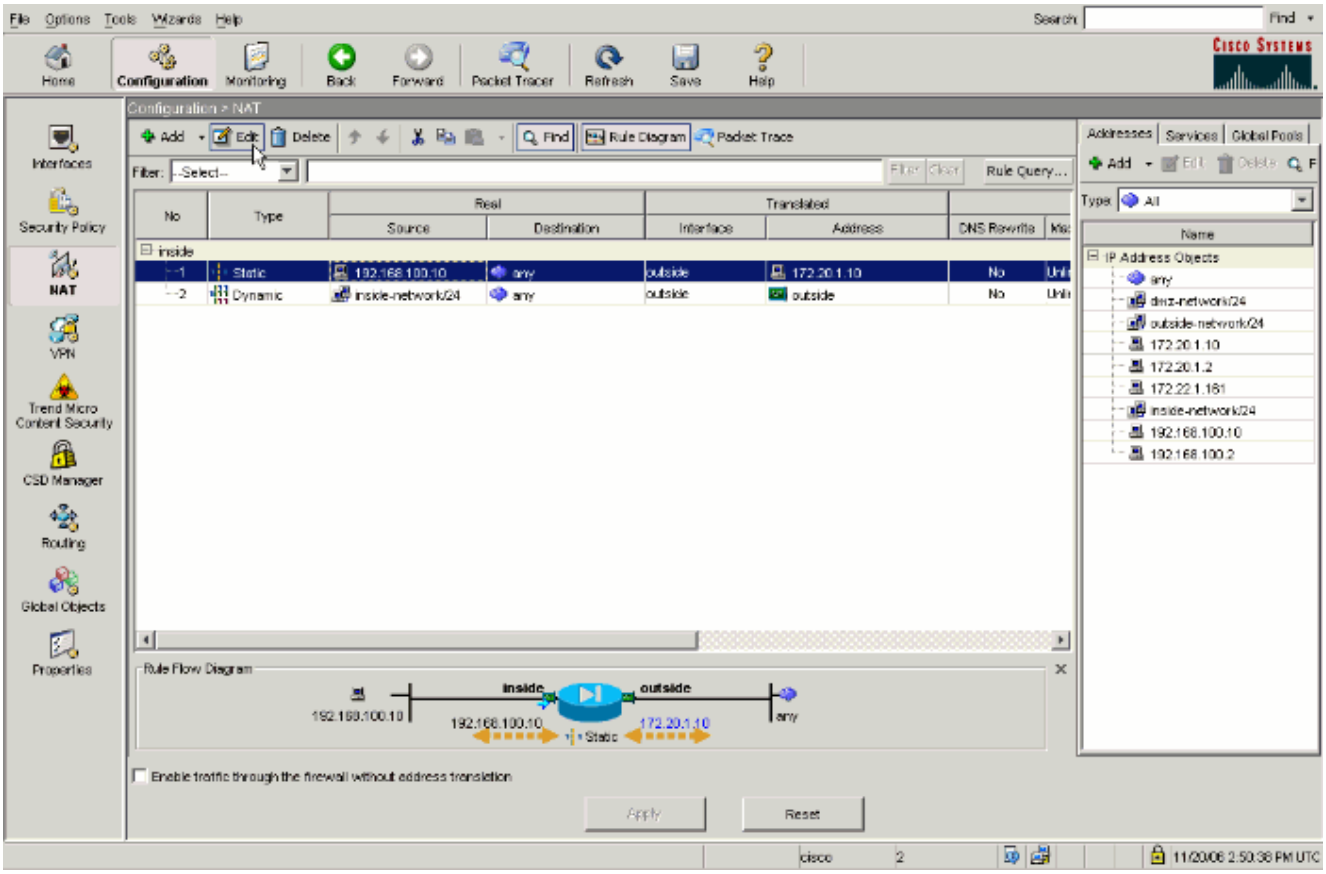
### 使用“dns”关键字进行 DNS 修正

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。如果正确配置了安全设备，安全设备则可以修改 A 记录，从而允许诸如问题：客户端无法访问 WWW 服务器部分中描述的这一类场景中的客户端进行连接。在这种情况下，DNS 修正处于启用状态，安全设备可以重写 A 记录以将客户端定向到 **192.168.100.10** 而不是 172.20.1.10。在将 **dns** 关键字添加到静态 NAT 语句时，会启用 DNS 修正。启用 DNS 修正后，配置的 NAT 部分如下所示：

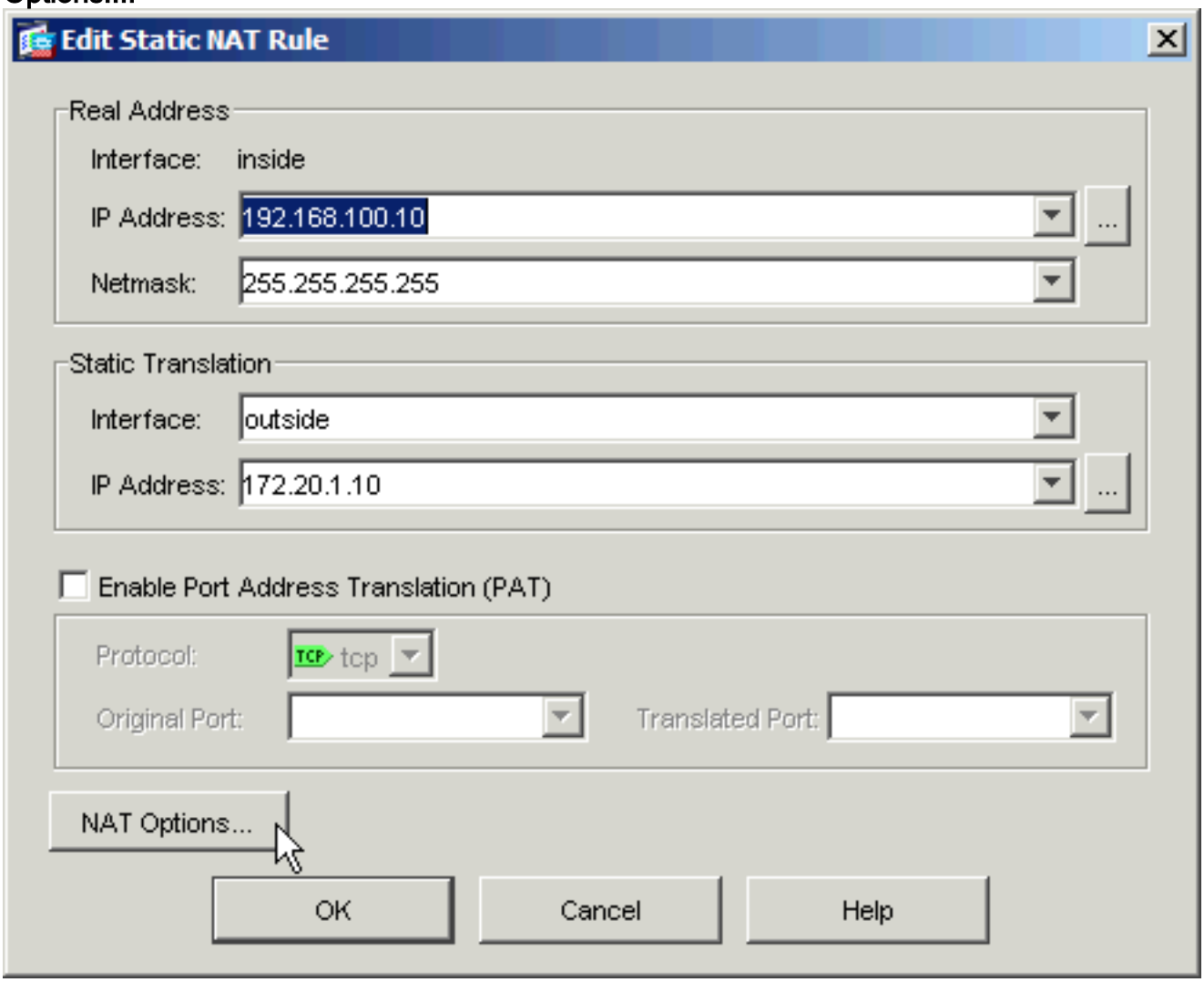
```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !--- Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0 static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns !--- The "dns" keyword is added to instruct the security appliance to modify !--- DNS records related to this entry. access-group OUTSIDE in interface outside !--- Output suppressed.
```

要在 ASDM 中配置 DNS 修正，请完成以下步骤：

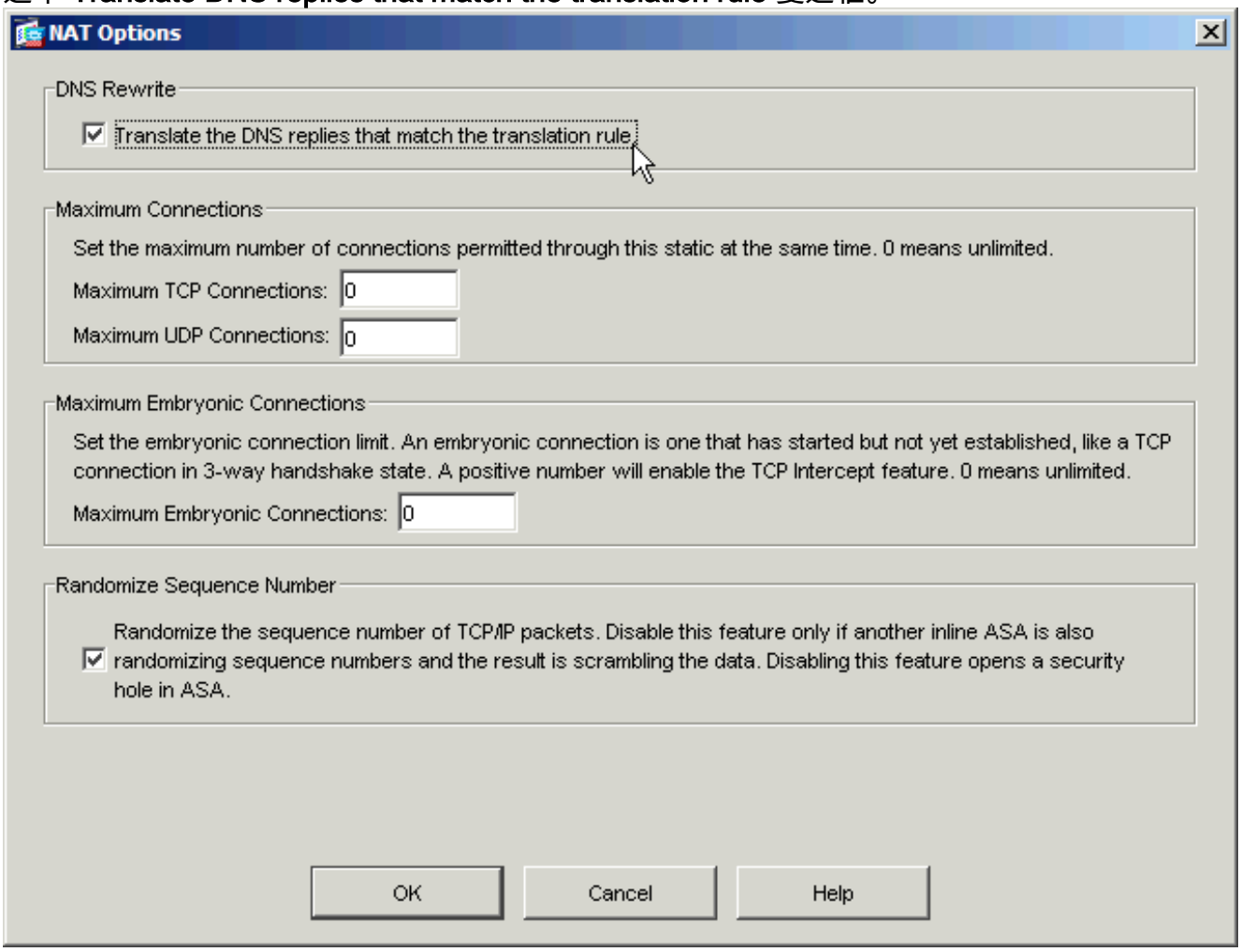
1. 导航到 **Configuration > NAT**，然后选择要进行修改的静态 NAT 规则。单击 **Edit**。




2. 单击 NAT Options....



3. 选中 **Translate DNS replies that match the translation rule** 复选框。




4. 单击 **OK** 退出“NAT Options”窗口。单击 **OK** 退出“Edit Static NAT Rule”窗口。单击 **Apply**，将您的配置发送到安全设备。

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
2 0.001251 **172.22.1.161 192.168.100.2 DNS Standard query response A 192.168.100.10** Frame 2 (94 bytes on wire, 94 bytes captured) Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00 (00:04:c0:c8:e4:00) Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2 (192.168.100.2) User Datagram Protocol, Src Port: domain (53), Dst Port: 52985 (52985) Domain Name System (response) [Request In: 1] [Time: 0.001251000 seconds] Transaction ID: 0x000c Flags: 0x8580 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001) **Answers server.example.com: type A, class IN, addr 192.168.100.10 Name: server.example.com Type: A (Host address) Class: IN (0x0001) Time to live: 1 hour Data length: 4 Addr: 192.168.100.10** *!--- 172.20.1.10 has been rewritten to be 192.168.100.10.*
5. 此时，客户端尝试访问地址为 192.168.100.10 的 WWW 服务器。连接成功。因为客户端和服务器位于同一个子网上，所以在 ASA 上未捕获到任何数据流。

## 使用“dns”关键字进行的最终配置

这是要使用 **dns** 关键字和两个 NAT 接口执行 DNS 修正的 ASA 的最终配置。

**最终 ASA 7.2(1) 配置**

```
ciscoasa(config)#show running-config : Saved : ASA
Version 7.2(1) ! hostname ciscoasa enable password
9jNfZuG3TC5tCVH0 encrypted names dns-guard ! interface
Ethernet0/0 nameif outside security-level 0 ip address
172.20.1.2 255.255.255.0 ! interface Ethernet0/1 nameif
inside security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address management-only ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list OUTSIDE extended
permit tcp any host 172.20.1.10 eq www !--- Simple
access-list that permits HTTP access to the mapped !---
address of the WWW server. pager lines 24 logging enable
logging buffered debugging mtu outside 1500 mtu inside
1500 asdm image disk0:/asdm512-k8.bin no asdm history
enable arp timeout 14400 global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 static
(inside,outside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 dns !--- PAT and static NAT
configuration. The DNS keyword instructs !--- the
security appliance to rewrite DNS records related to
this entry. access-group OUTSIDE in interface outside !-
-- The Access Control List (ACL) that permits HTTP
access !--- to the WWW server is applied to the outside
interface. route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
```

```
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns MY_DNS_INSPECT_MAP parameters message-length maximum
512 !--- DNS inspection map. policy-map global_policy
class inspection_default inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp inspect
dns MY_DNS_INSPECT_MAP !--- DNS inspection is enabled
using the configured map. inspect icmp policy-map type
inspect dns migrated_dns_map_1 parameters message-length
maximum 512 ! service-policy global_policy global prompt
hostname context
Cryptochecksum:a4a38088109887c3ceb481efab3dcf32 : end
```

## 备用解决方案：发夹

### 采用静态 NAT 的发夹

**警告：** 采用静态 NAT 的发夹涉及通过安全设备发送客户端和 WWW 服务器之间的所有数据流。实施此解决方案之前，请仔细考虑期望的数据流量和您的安全设备的功能。

发夹是指从数据流发送至的接口上发送回数据流的过程。在安全设备软件 7.0 版中引入了此功能。对于 7.2(1) 之前的版本，要求至少加密一手臂的发夹的流量（入站或出站）。在 7.2(1) 及更高版本中，此要求不再适用。使用 7.2(1) 时，入站流量和出站流量可能会被同时解密。

结合了静态 NAT 语句的发夹，可用于获得与 DNS 修正相同的效果。此方法不会更改从 DNS 服务器返回到客户端的 DNS A 记录的内容。然而，使用发夹功能时（例如本文档中讨论的场景），客户端可以使用由 DNS 服务器返回的地址 **172.20.1.10** 进行连接。

使用发夹和静态 NAT 以获得 DNS 修正效果时，配置的相关部分如下所示。在该输出的结尾部分较为详细地说明了以粗体显示的命令：

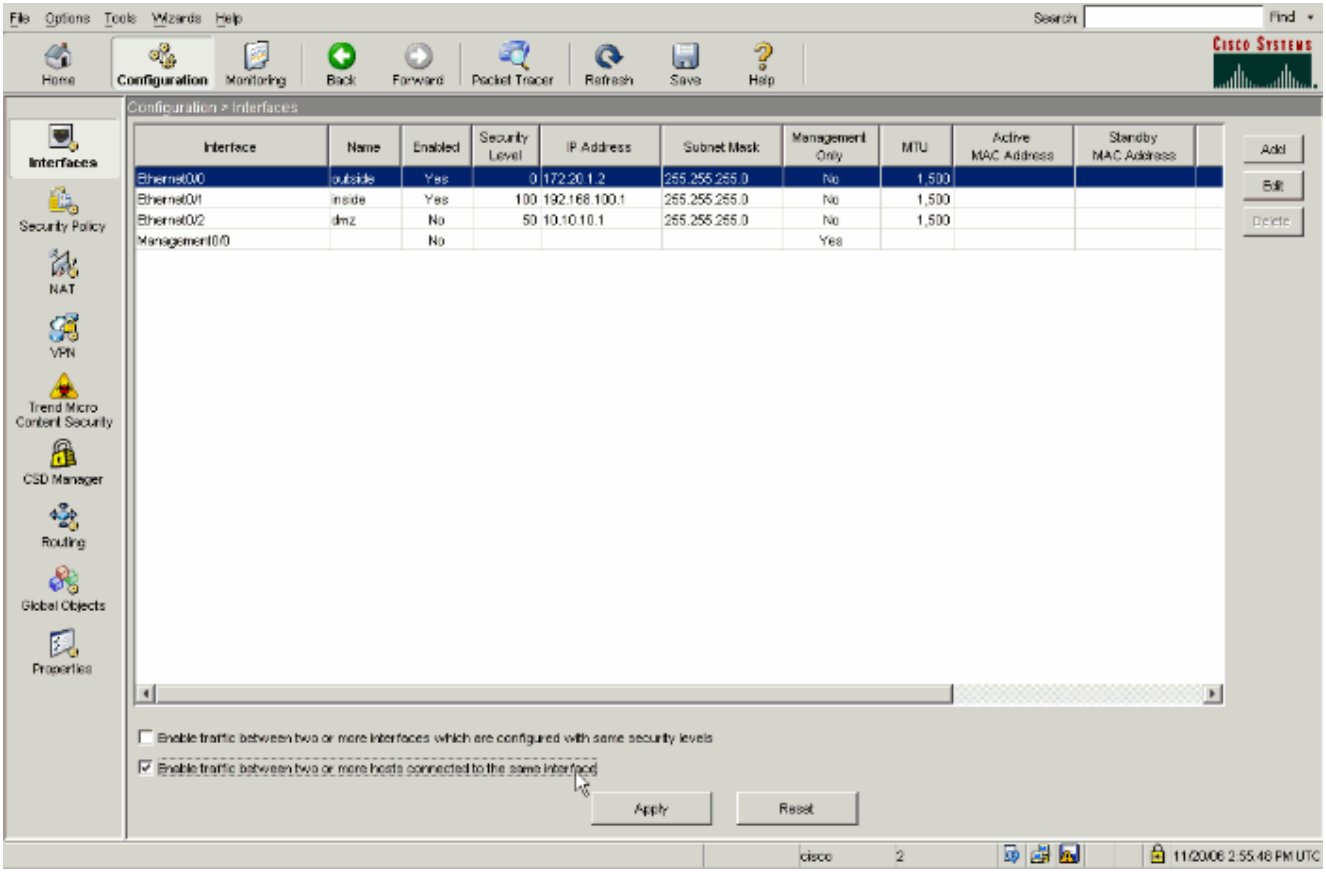
```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. same-security-traffic permit intra-interface !--- Enable hairpinning. global
(outside) 1 interface !--- Global statement for client access to the Internet. global (inside) 1
interface !--- Global statment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

- **same-security-traffic** — 通过此命令，相同安全级别的流量可以传输安全设备。**permit intra-interface** 关键字允许 same-security-traffic 进入和离开同一接口，从而启用发夹功能。**注意**：有关发夹和 **same-security-traffic** 命令的详细信息，请参阅 same-security-traffic。
- **global (inside) 1 interface** — 通过安全设备的所有流量必须经过 NAT。此命令使用安全设备的内部接口地址，以使进入内部接口的流量在通过发夹功能从内部接口发送回时经过 PAT。
- **static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255** — 此静态 NAT 条目为 WWW 服务器的公用 IP 地址创建第二个映射。但是，与第一个静态 NAT 条目不同，这次，地址 172.20.1.10 将映射到安全设备的内部接口。这允许安全设备响应在内部接口的此地址

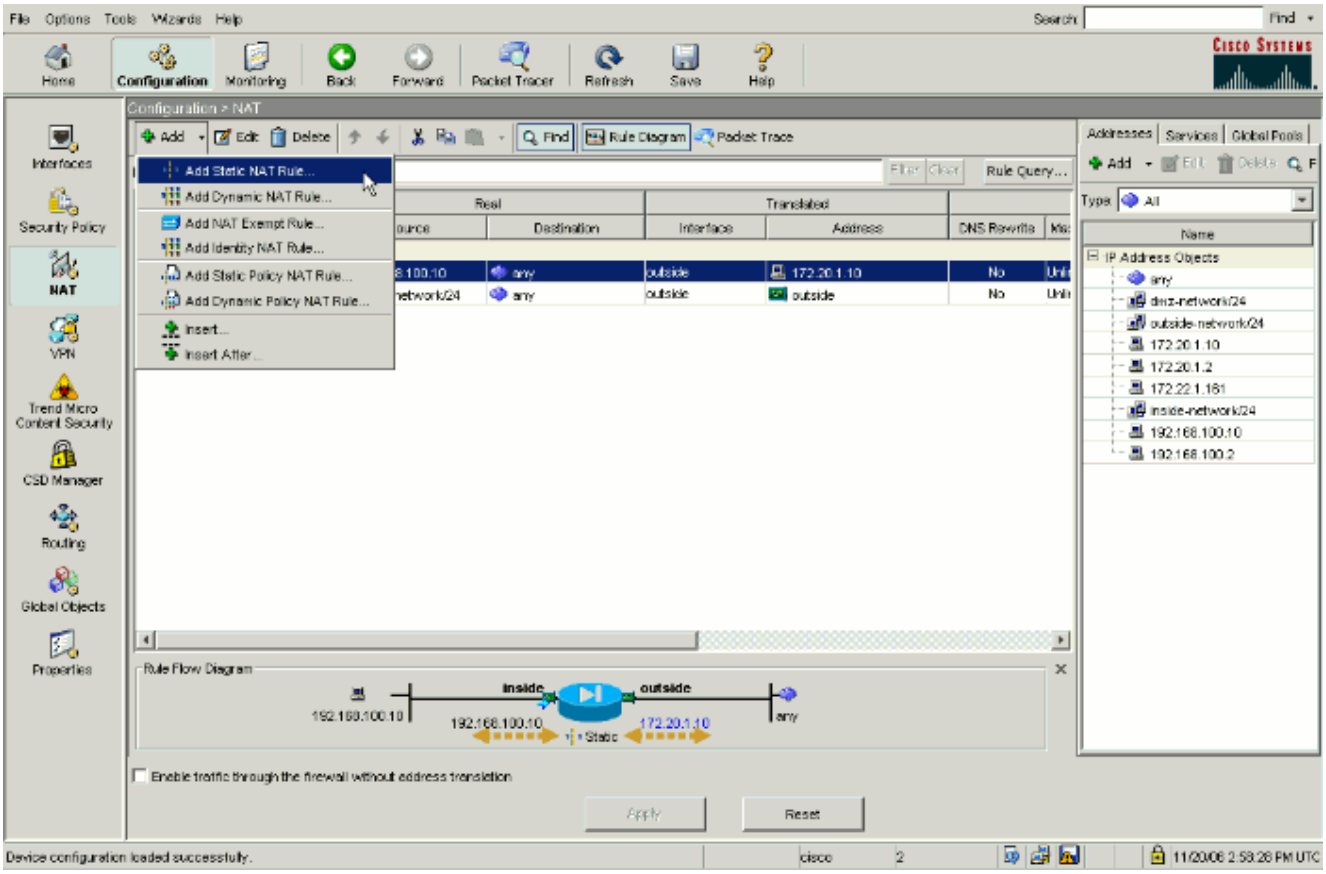
看到的请求。然后，它通过自身将那些请求重定向到 WWW 服务器的实际地址。

要在 ASDM 中配置采用静态 NAT 的发夹，请完成以下步骤：

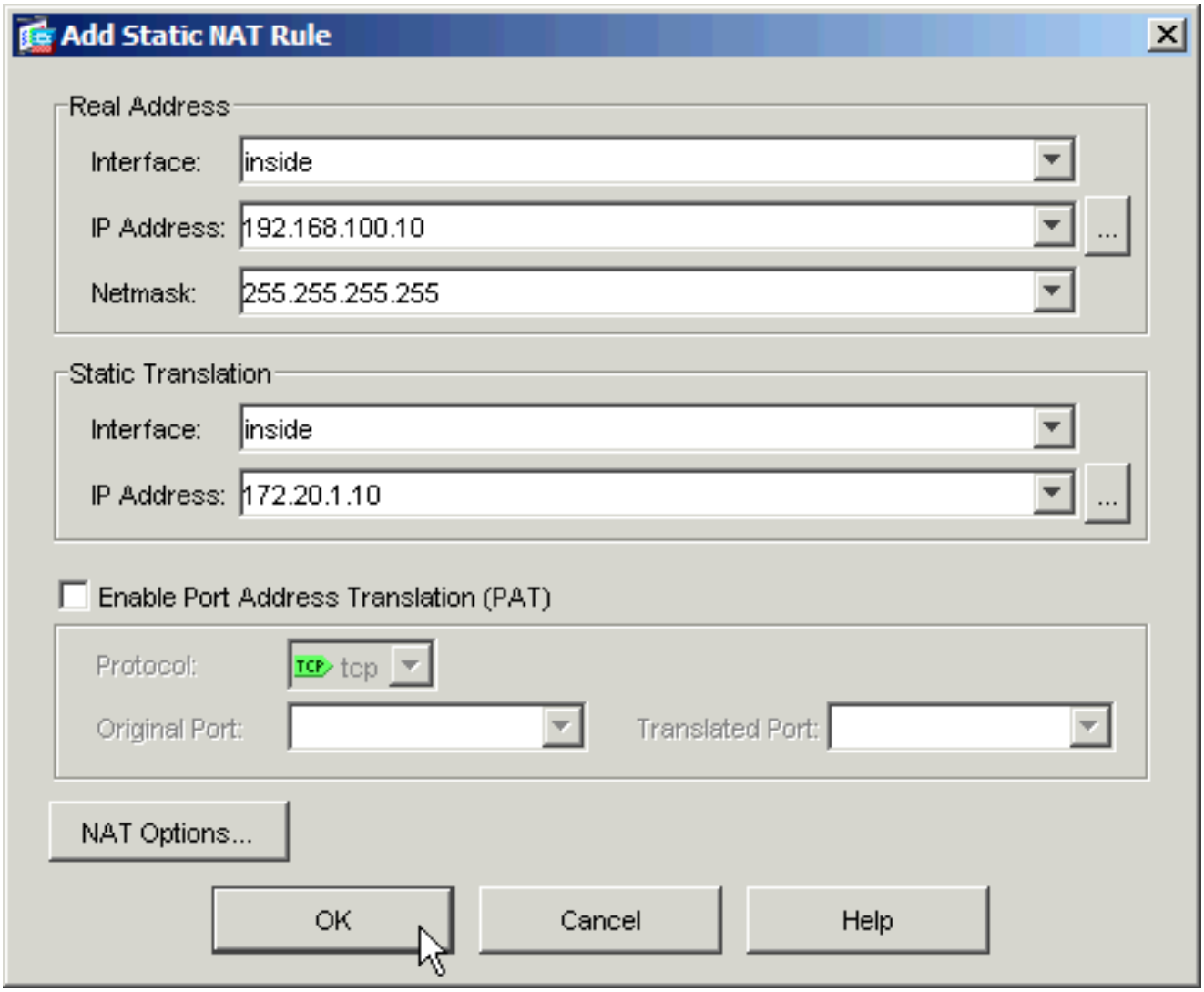
1. 导航到 **Configuration > Interfaces**。
2. 在窗口底部，选中 **Enable traffic between two or more hosts connected to the same interface** 复选框。



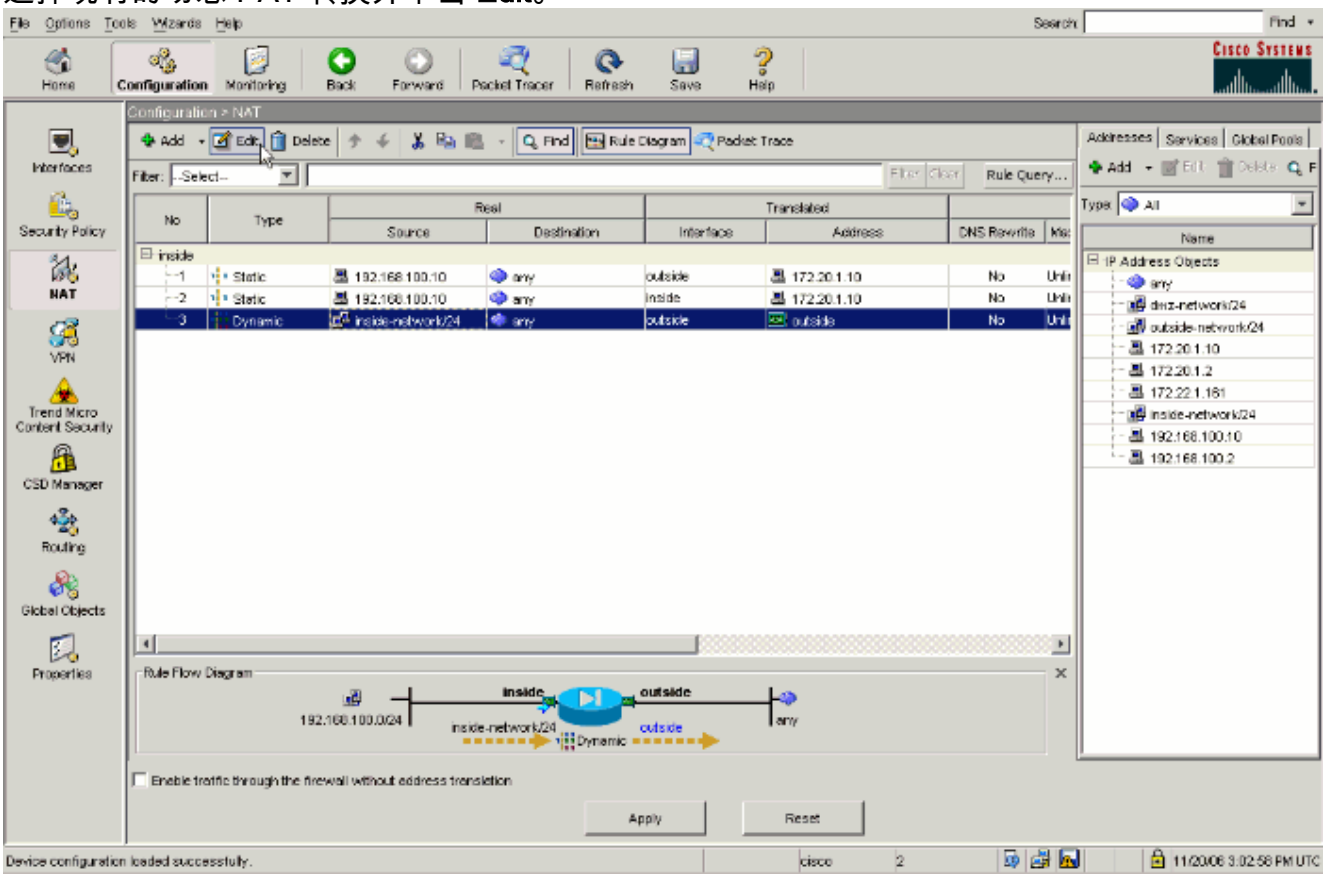

3. 单击 **Apply**。
4. 导航到 **Configuration > NAT**，然后选择“Add”>“Add Static NAT Rule....”



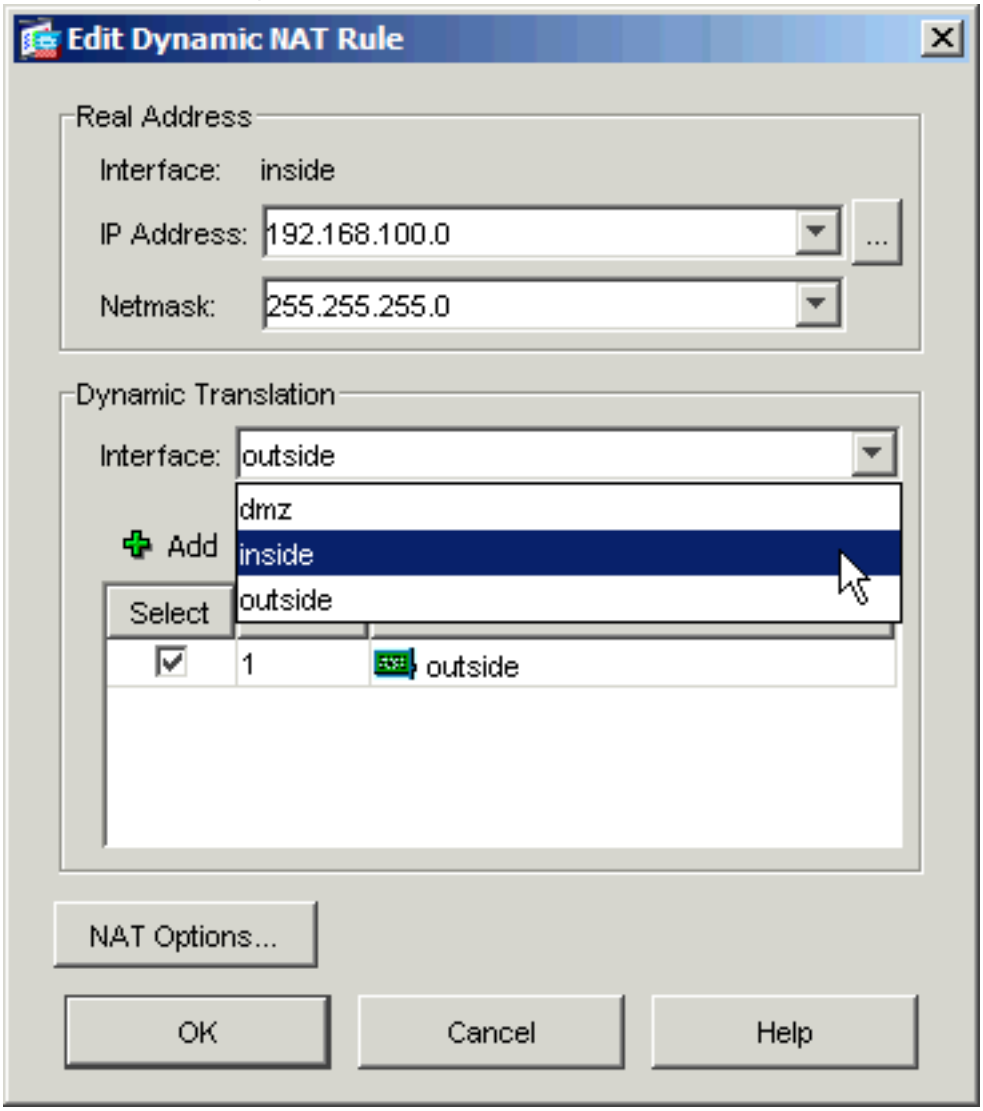

5. 填写新静态转换的配置。用 WWW 服务器的信息填充 **Real Address** 区域。用要将 WWW 服务器映射到的地址和接口填充 **Static Translation** 区域。在这种情况下，选择内部接口以允许内部接口上的主机通过映射的地址 172.20.1.10 访问 WWW 服务器。

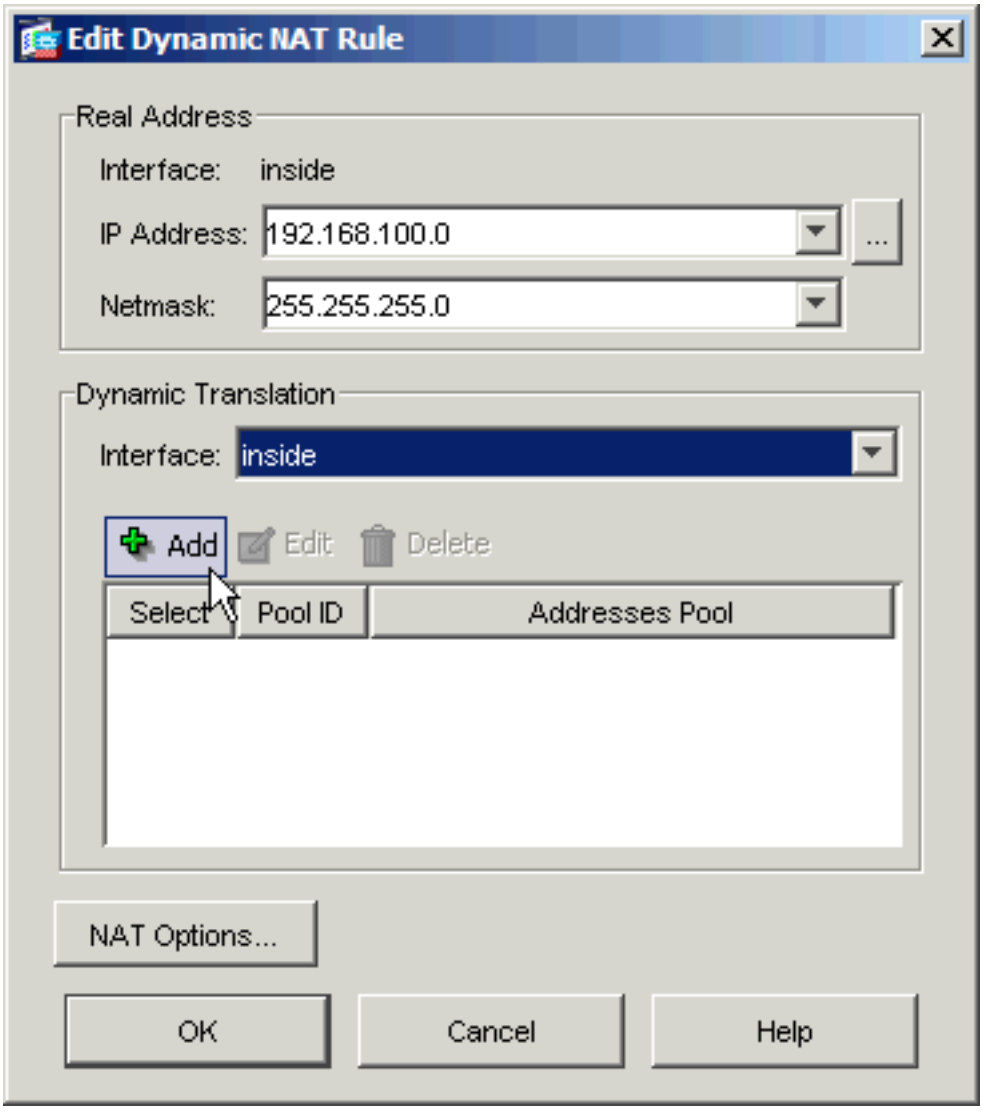



6. 单击 **OK** 退出“Add Static NAT Rule”窗口。
7. 选择现有的动态 PAT 转换并单击 **Edit**。

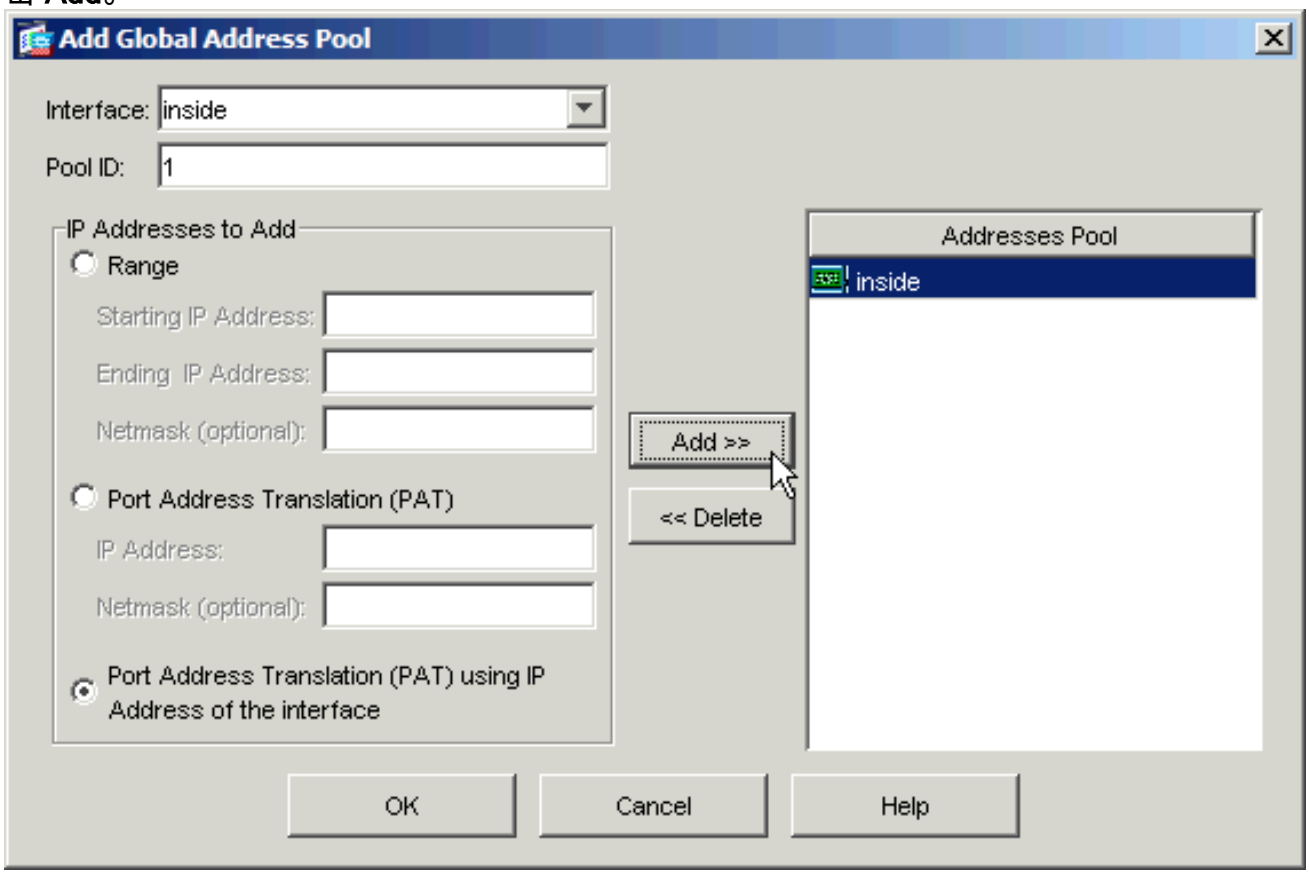


8. 从“Interface”下拉框中选择 **inside**。






9. 单击 **Add**。
10. 选择标有 **Port Address Translation (PAT) using IP address of the interface** 的单选按钮。单击 **Add**。



11. 单击 **OK** 退出“Add Global Address Pool”窗口。单击 **OK** 退出“Edit Dynamic NAT Rule”窗口。单击 **Apply**，将您的配置发送到安全设备。

以下是配置发夹时事件的发生顺序。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确定 WWW 服务器的地址是否为 192.168.100.10。`%ASA-7-609001: Built local-host inside:192.168.100.10`
3. 安全设备将为客户端创建一个动态 PAT 转换。现在，客户端数据流的来源是安全设备（地址为 192.168.100.1）的192.168.100.1。`%ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to inside:`**`192.168.100.1/1026`**
4. 安全设备通过自身在客户端和 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 inbound TCP connection 67399 for inside:192.168.100.2/11012` **`(192.168.100.1/1026)`** `to inside:192.168.100.10/80` **`(172.20.1.10/80)`**
5. 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。`ciscoasa(config)#`**`show xlate`** `3 in use, 9 most used Global 172.20.1.10 Local 192.168.100.10 Global 172.20.1.10 Local 192.168.100.10` **`PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)`**
6. 安全设备上的 **show conn** 命令可验证是否已在安全设备和代表客户端的 WWW 服务器之间成功建立了连接。请注意括号内客户端的实际地址。`ciscoasa#`**`show conn`** `TCP out 192.168.100.1`**`(192.168.100.2)`**`:11019 in 192.168.100.10:80 idle 0:00:03 bytes 1120 flags UIOB`

## 使用发夹和静态 NAT 设置的最终配置

这是使用发夹和静态 NAT 获得 DNS 修正效果（通过两个 NAT 接口实现）的 ASA 的最终配置。

**最终 ASA 7.2(1) 配置**

```
ciscoasa(config-if)#show running-config : Saved : ASA
Version 7.2(1) ! hostname ciscoasa enable password
9jNfZuG3TC5tCVH0 encrypted names dns-guard ! interface
Ethernet0/0 nameif outside security-level 0 ip address
172.20.1.2 255.255.255.0 ! interface Ethernet0/1 nameif
inside security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address management-only ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive same-security-traffic permit
intra-interface access-list OUTSIDE extended permit tcp
any host 172.20.1.10 eq www !--- Simple access-list that
permits HTTP access to the mapped !--- address of the
WWW server. pager lines 24 logging enable logging
buffered debugging mtu outside 1500 mtu inside 1500 asdm
image disk0:/asdm512-k8.bin no asdm history enable arp
timeout 14400 global (outside) 1 interface !--- Global
statement for client access to the Internet. global
(inside) 1 interface !--- Global statment for hairpinned
client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT
statement defines which traffic should be natted. !---
The whole inside subnet in this case. static
(inside,outside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 !--- Static NAT statement mapping the
WWW server's real address to a public !--- address on
the outside interface. static (inside,inside)
```

```
172.20.1.10 192.168.100.10 netmask 255.255.255.255 !---
Static NAT statement mapping requests for the public IP
address of the !--- WWW server that appear on the inside
interface to the WWW server's real address !--- of
192.168.100.10. access-group OUTSIDE in interface
outside !--- The ACL that permits HTTP access to the WWW
server is applied !--- to the outside interface. route
outside 0.0.0.0 0.0.0.0 172.20.1.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns MY_DNS_INSPECT_MAP parameters message-length maximum
512 policy-map global_policy class inspection_default
inspect ftp inspect h323 h225 inspect h323 ras inspect
rsh inspect rtsp inspect esmtp inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:7c9b4e3aff085ba90ee194e079111e1d
: end
```

**注意：** 参考此视频，在思科ASA ( 仅限注册用户)的发夹，关于可能使用两隧道间的本地交换的不同的方案的更多信息。

## 配置 DNS 检查

为了启用 DNS 检查（如果以前被禁用），请执行以下步骤。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。有关服务策略和检查的详细信息，请参阅使用模块化策略框架。

1. 为 DNS 创建检查策略映射。`ciscoasa(config)#`**`policy-map type inspect dns MY_DNS_INSPECT_MAP`**
2. 在策略映射配置模式下，进入参数配置模式以便为检测引擎指定参数。`ciscoasa(config-pmap)#`**`parameters`**
3. 在策略映射参数配置模式下，将 DNS 消息的最大消息长度指定为 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. 在策略映射类配置模式下，指定应该使用在步骤 1-3 中创建的检查策略映射来检查 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
```

# 分割 DNS 配置

在组策略配置模式下发出 **split-dns** 命令，以进入要通过分割隧道解析的域列表。使用此命令的 ***no 形式*** 删除列表。

在没有分割隧道域列表的情况下，用户将继承默认组策略中存在的任何内容。发出 **split-dns none** 命令以防止继承分割隧道域列表。

使用一个空格来分隔域列表中的各个条目。条目的数量没有限制，但整个字符串的长度不得超过 255 个字符。只能使用字母数字字符、连字符 (-) 和句点 (.)。不带任何参数使用 **no split-dns** 命令时，删除所有当前值，包括发出 split-dns none 命令时创建的空值。

本示例演示了如何配置域 Domain1、Domain2、Domain3 和 Domain4，以便针对 FirstGroup 组策略通过分割隧道来解析这些域：

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

# 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。请参阅配置 DNS 检查部分。

## 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 dmz:10.10.10.10/23
```

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。

## 丢弃 UDP DNS 应答

您可能因丢弃了 DNS 数据包而收到以下错误消息：

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

在 512-65535 之间增加 DNS 数据包长度以解决此问题。

**示例：**

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

# 相关信息

- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品售后通知
- 请求注解 (RFC)
- 在思科ASA的发夹连接
- Cisco ASA 5500 系列自适应安全设备

- 技术支持和文档 - Cisco Systems