

在ASA后查找其公有IP地址的主机之间的LAN通信

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题：在ASA后查找其公有IP地址的主机之间的LAN通信](#)

[示例1.源主机PC-A连接到内部ASA接口，而目标主机测试服务器连接到DMZ接口。](#)

[示例2.源主机和目的主机PC-A和测试服务器连接到同一个内部ASA接口。](#)

[示例3.源主机和目的主机PC-A和测试服务器连接到内部ASA接口，但位于另一第3层设备后面（可以是路由器或多层交换机）。](#)

[解决方案](#)

[示例1.源主机PC-A连接到内部ASA接口，而目标主机测试服务器连接到DMZ接口。](#)

[配置](#)

[故障排除](#)

[示例2.源主机和目的主机PC-A和测试服务器连接到同一个内部ASA接口。](#)

[配置](#)

[故障排除](#)

[示例3.源主机和目的主机PC-A和测试服务器连接到内部ASA接口，但位于另一第3层设备后面（可以是路由器或多层交换机）。](#)

[配置](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍不同的网络实施，从而允许在自适应安全设备(ASA)后查找其公有IP地址的主机之间进行局域网(LAN)通信。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科基本ASA NAT配置，版本8.3及更高版本。
- 思科基本ASA NAT配置，版本8.2及更早。

使用的组件

本文档中的信息基于以下软件和硬件版本：

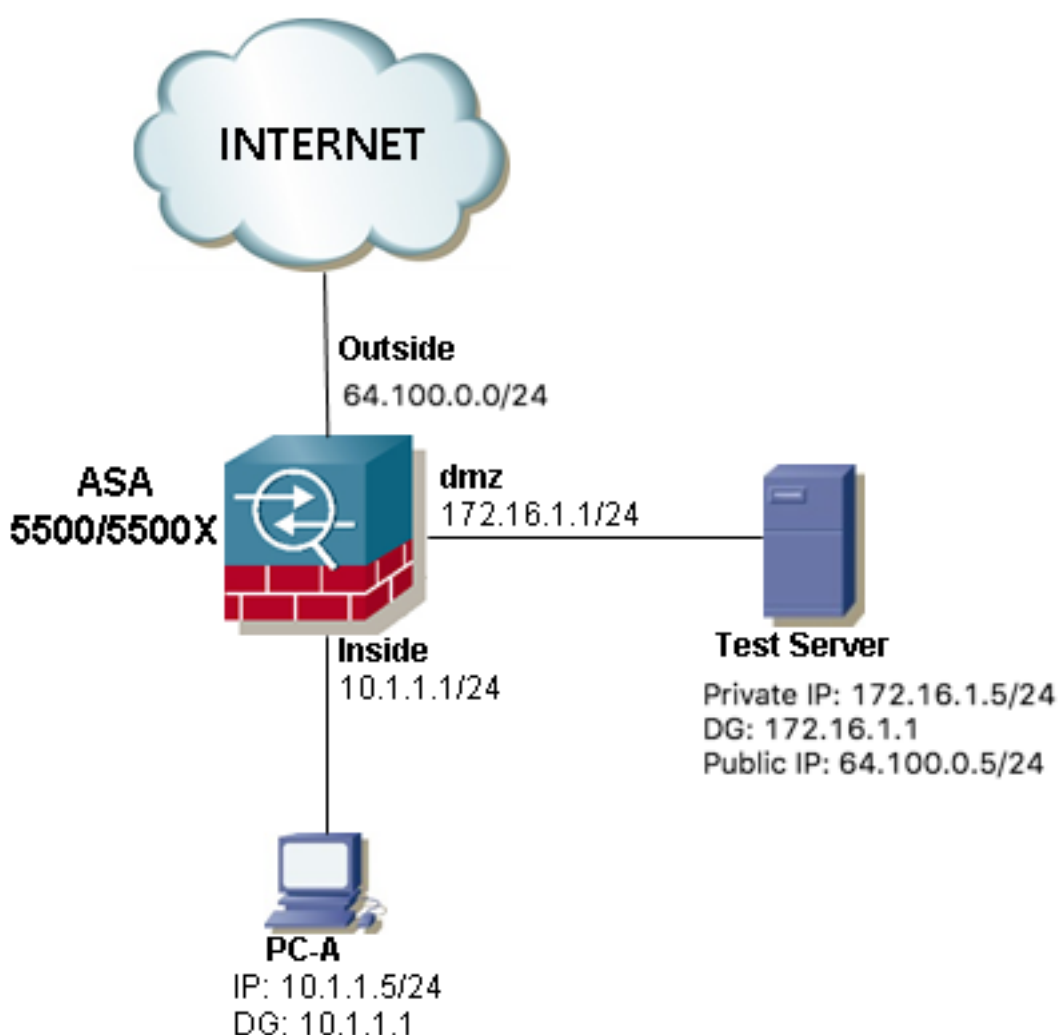
- ASA5500和ASA5500-X系列。
- Cisco ASA 8.3及更高版本。
- Cisco ASA 8.2及更高版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

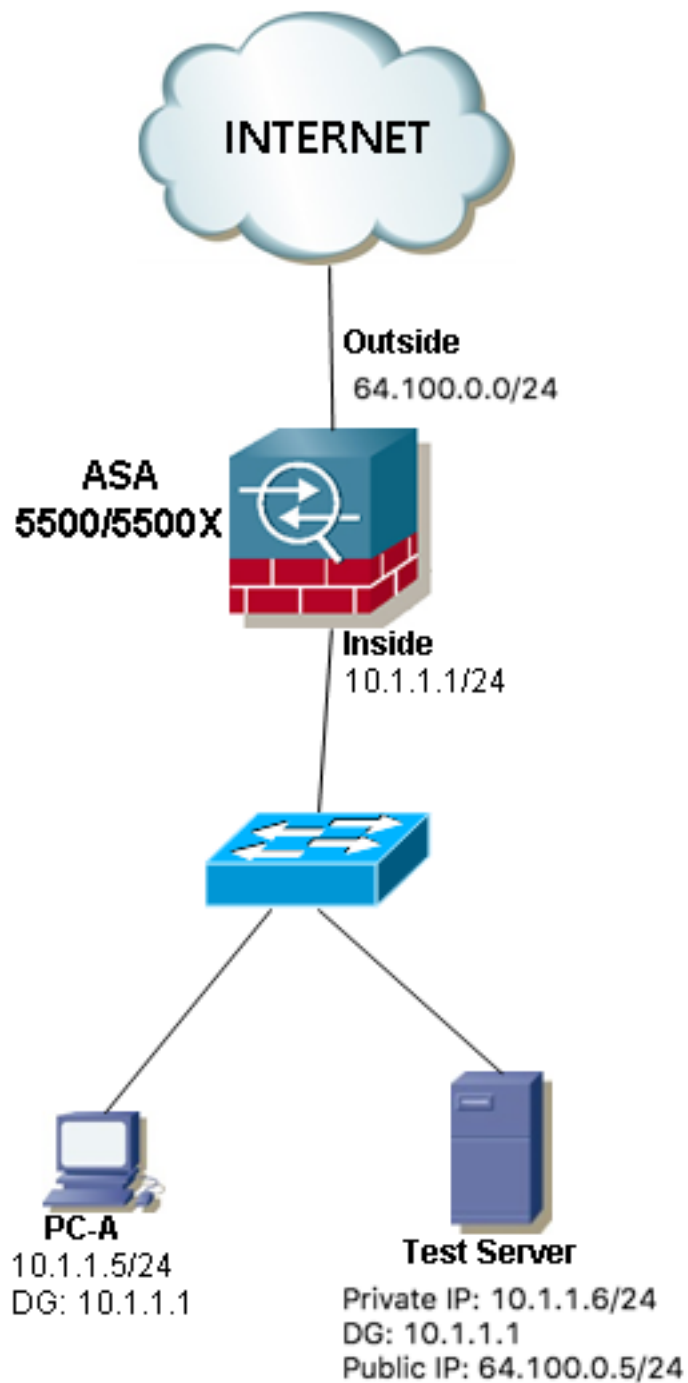
问题：在ASA后查找其公有IP地址的主机之间的LAN通信

在下一节中，您可以看到三个拓扑示例，这些示例显示了此通信要求，允许在ASA后查找其公有IP地址的主机之间进行LAN通信。

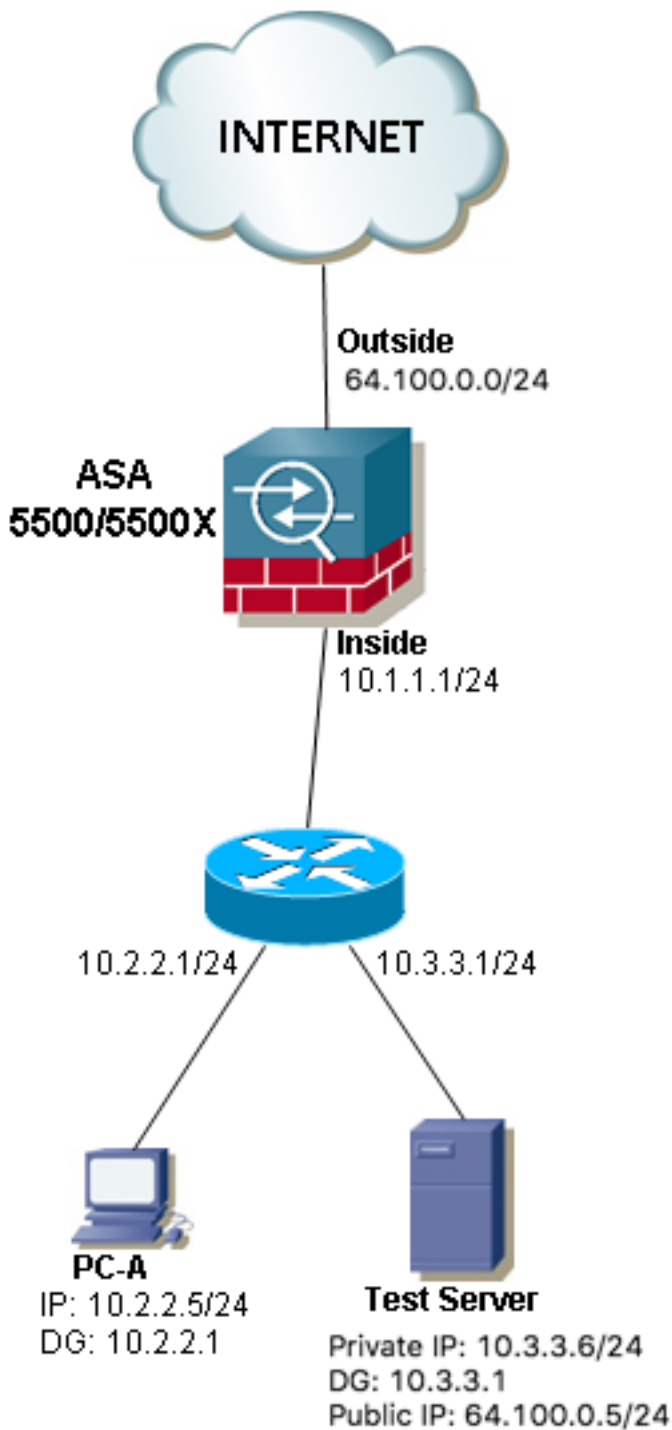
示例1.源主机PC-A连接到内部ASA接口，而目标主机测试服务器连接到DMZ接口。



示例2.源主机和目的主机PC-A和测试服务器连接到同一个内部ASA接口。



示例3.源主机和目的主机PC-A和测试服务器连接到内部ASA接口，但位于另一第3层设备后面（可以是路由器或多层交换机）。



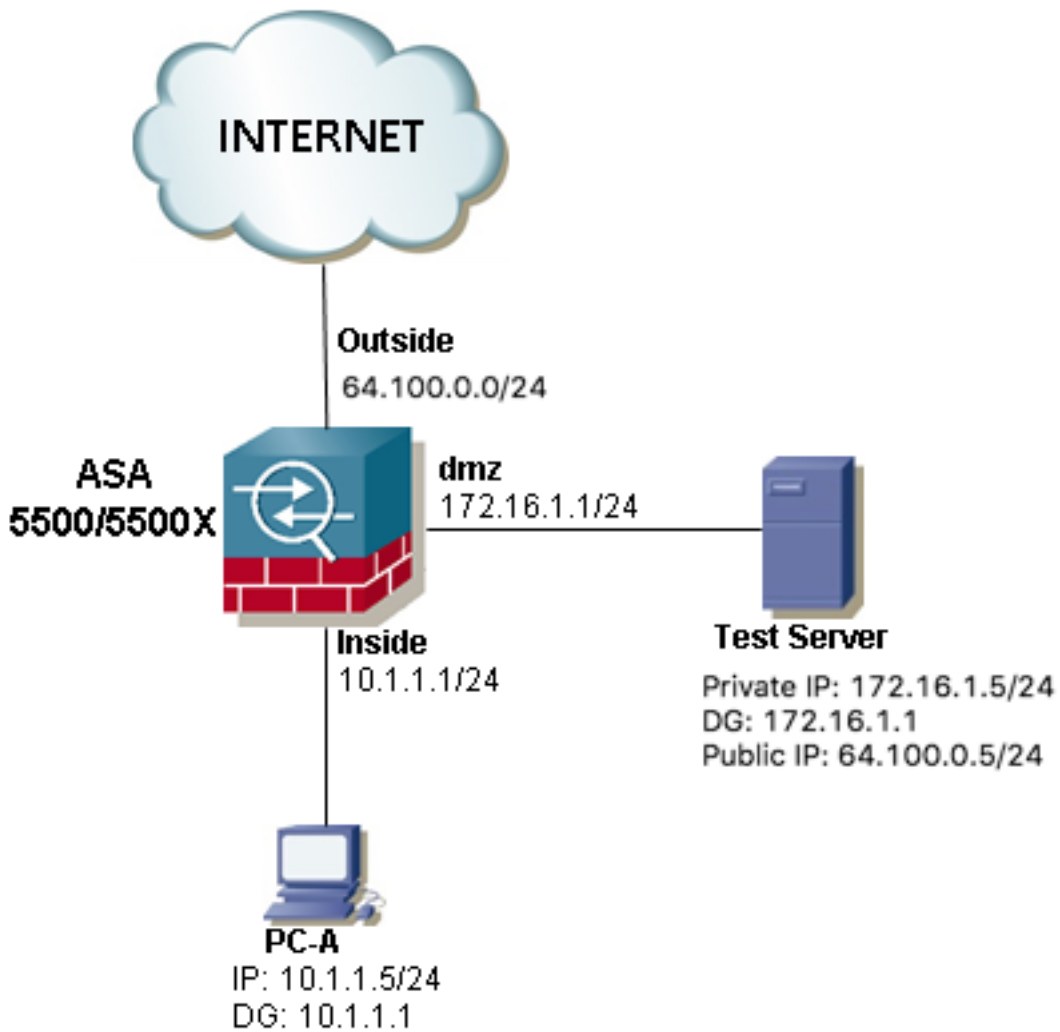
注意：三个映像中的**测试服务器**在ASA中配置了静态网络地址转换(NAT)，此静态NAT转换从外部应用到相应的内部接口，以便允许从公有IP地址为64.100.0.5的外部访问**测试服务器**，然后转换为**测试服务器**内部私有IP地址。

解决方案

为了允许源主机PC-A使用其公有IP地址而非私有IP地址到达目的测试服务器，我们需要应用两次NAT配置。两次NAT配置有助于我们在流量通过ASA时转换数据包的源IP地址和目的IP地址。

下面是每个拓扑所需的两次nat配置的详细信息：

示例1.源主机PC-A连接到内部ASA接口，而目标主机测试服务器连接到DMZ接口。



配置

ASA 8.3及更高版本的两次NAT:

```
object network obj-10.1.1.5  
host 10.1.1.5
```

```
object network obj-172.16.1.5  
host 172.16.1.5
```

```
object network obj-64.100.0.5  
host 64.100.0.5
```

```
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-172.16.1.5
```

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.

ASA 8.2及更早版本的两次NAT:

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.1.1.5 host 64.100.0.5
static (inside,dmz) interface access-list IN-DMZ-INTERFACE
```

```
access-list DMZ-IN-INTERFACE extended permit ip host 172.16.1.5 host 172.16.1.1
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
```

故障排除

Packet Tracer输出版本8.3及更高版本：

```
ASA# packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80
```

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-172.16.1.5
```

Additional Information:

NAT divert to egress interface dmz

Untranslate 64.100.0.5/80 to 172.16.1.5/80

Phase: 3

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-172.16.1.5
```

Additional Information:

Static translate 10.1.1.5/123 to 172.16.1.1/123

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-172.16.1.5
```

Additional Information:

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 167632, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: dmz

output-status: up

output-line-status: up

Action: allow

Packet Tracer输出版本8.2及更低版本：

```
ASA#packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80
```

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
```

```
match ip dmz host 172.16.1.5 inside host 172.16.1.1
```

```
static translation to 64.100.0.5
```

```
translate_hits = 0, untranslate_hits = 1
```

Additional Information:

NAT divert to egress interface dmz

Untranslate 64.100.0.5/0 to 172.16.1.5/0 using netmask 255.255.255.255

Phase: 2

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 3

Type: NAT

Subtype:

Result: ALLOW

Config:

```
static (inside,dmz) interface access-list IN-DMZ-INTERFACE
match ip inside host 10.1.1.5 dmz host 64.100.0.5
static translation to 172.16.1.1
translate_hits = 1, untranslate_hits = 0
```

Additional Information:

Static translate 10.1.1.5/0 to 172.16.1.1/0 using netmask 255.255.255.255

Phase: 4

Type: NAT

Subtype: host-limits

Result: ALLOW

Config:

```
static (inside,dmz) interface access-list IN-DMZ-INTERFACE
match ip inside host 10.1.1.5 dmz host 64.100.0.5
static translation to 172.16.1.1
translate_hits = 1, untranslate_hits = 0
```

Additional Information:

Phase: 5

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
match ip dmz host 172.16.1.5 inside host 172.16.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
```

Additional Information:

Phase: 6

Type: NAT

Subtype: host-limits

Result: ALLOW

Config:

```
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
match ip dmz host 172.16.1.5 inside host 172.16.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
```

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 503, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: dmz

output-status: up

output-line-status: up

Action: allow

数据包捕获：

```
ASA# sh cap
capture capin type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.5 host 64.100.0.5
capture capout type raw-data interface dmz [Capturing - 1300 bytes]
match ip host 172.16.1.1 host 172.16.1.5
```

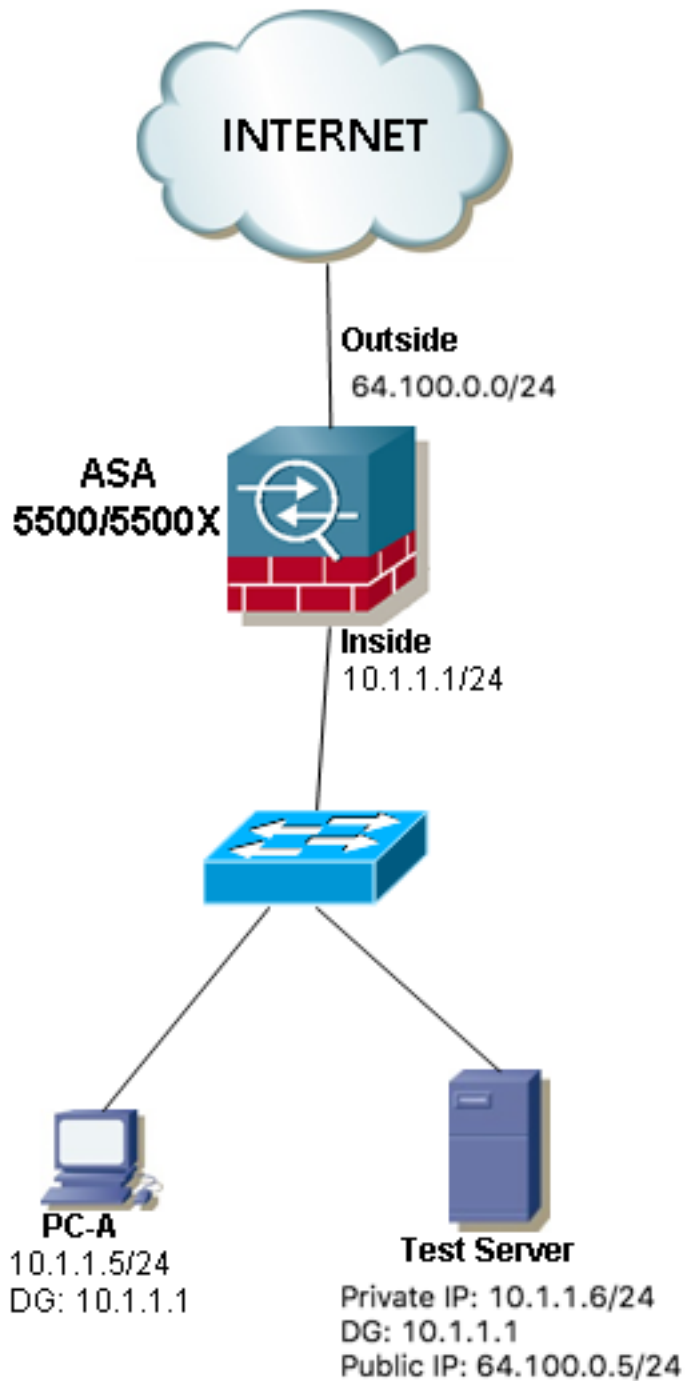
```
ASA# sh cap capin
```

```
10 packets captured
1: 12:36:28.245455 10.1.1.5 > 64.100.0.5: icmp: echo request
2: 12:36:28.269441 64.100.0.5 > 10.1.1.5: icmp: echo reply
3: 12:36:28.303451 10.1.1.5 > 64.100.0.5: icmp: echo request
4: 12:36:28.333692 64.100.0.5 > 10.1.1.5: icmp: echo reply
5: 12:36:28.372478 10.1.1.5 > 64.100.0.5: icmp: echo request
6: 12:36:28.395563 64.100.0.5 > 10.1.1.5: icmp: echo reply
7: 12:36:28.422402 10.1.1.5 > 64.100.0.5: icmp: echo request
8: 12:36:28.449241 64.100.0.5 > 10.1.1.5: icmp: echo reply
9: 12:36:28.481420 10.1.1.5 > 64.100.0.5: icmp: echo request
10: 12:36:28.507435 64.100.0.5 > 10.1.1.5: icmp: echo reply
10 packets shown
```

```
ASA1# sh cap capout
```

```
10 packets captured
1: 12:36:28.245730 172.16.1.1 > 172.16.1.5: icmp: echo request
2: 12:36:28.269395 172.16.1.5 > 172.16.1.1: icmp: echo reply
3: 12:36:28.303725 172.16.1.1 > 172.16.1.5: icmp: echo request
4: 12:36:28.333646 172.16.1.5 > 172.16.1.1: icmp: echo reply
5: 12:36:28.372737 172.16.1.1 > 172.16.1.5: icmp: echo request
6: 12:36:28.395533 172.16.1.5 > 172.16.1.1: icmp: echo reply
7: 12:36:28.422661 172.16.1.1 > 172.16.1.5: icmp: echo request
8: 12:36:28.449195 172.16.1.5 > 172.16.1.1: icmp: echo reply
9: 12:36:28.481695 172.16.1.1 > 172.16.1.5: icmp: echo request
10: 12:36:28.507404 172.16.1.5 > 172.16.1.1: icmp: echo reply
10 packets shown
```

示例2.源主机和目的主机PC-A和测试服务器连接到同一个内部ASA接口。



配置

ASA 8.3及更高版本的两次NAT:

```
object network obj-10.1.1.5  
host 10.1.1.5
```

```
object network obj-10.1.1.6  
host 10.1.1.6
```

```
object network obj-64.100.0.5  
host 64.100.0.5
```

```
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-  
10.1.1.6
```

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.

ASA 8.2及更早版本的两次NAT:

```
access-list IN-OUT-INTERFACE extended permit ip host 10.1.1.5 host 64.100.0.5  
static (inside,inside) interface access-list IN-OUT-INTERFACE
```

```
access-list OUT-IN-INTERFACE extended permit ip host 10.1.1.6 host 10.1.1.1  
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
```

注意：源IP地址从10.1.1.5转换到ASA内部接口IP地址10.1.1.1的NAT转换的主要目的是强制来自主机10.1.1.6的应答返回到ASA，这是避免非对称路由和允许ASA处理所有流量的高要求感兴趣的主机，如果我们不像本例中那样转换源IP地址，则ASA将因非对称路由而阻止感兴趣的流量。

故障排除

Packet Tracer输出版本8.3及更高版本：

```
ASA# packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80
```

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-10.1.1.6
```

Additional Information:

NAT divert to egress interface inside

Untranslate 64.100.0.5/80 to 10.1.1.6/80

Phase: 2

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-10.1.1.6
```

Additional Information:

Static translate 10.1.1.5/123 to 10.1.1.1/123

Phase: 3

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-10.1.1.6
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 167839, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow

Packet Tracer输出版本8.2及更低版本：

```
ASA# packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80
```

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.1.1.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:
NAT divert to egress interface inside

Untranslate 64.100.0.5/0 to 10.1.1.6/0 using netmask 255.255.255.255

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.1.1.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.1.1.5/0 to 10.1.1.1/0 using netmask 255.255.255.255

Phase: 5
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.1.1.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.1.1.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 7
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.1.1.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 8
Type: IP-OPTIONS

Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:

Additional Information:
New flow created with id 727, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow

数据包捕获：

```
ASA# sh cap
capture capin type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.5 host 64.100.0.5
capture capout type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.1 host 10.1.1.6
```

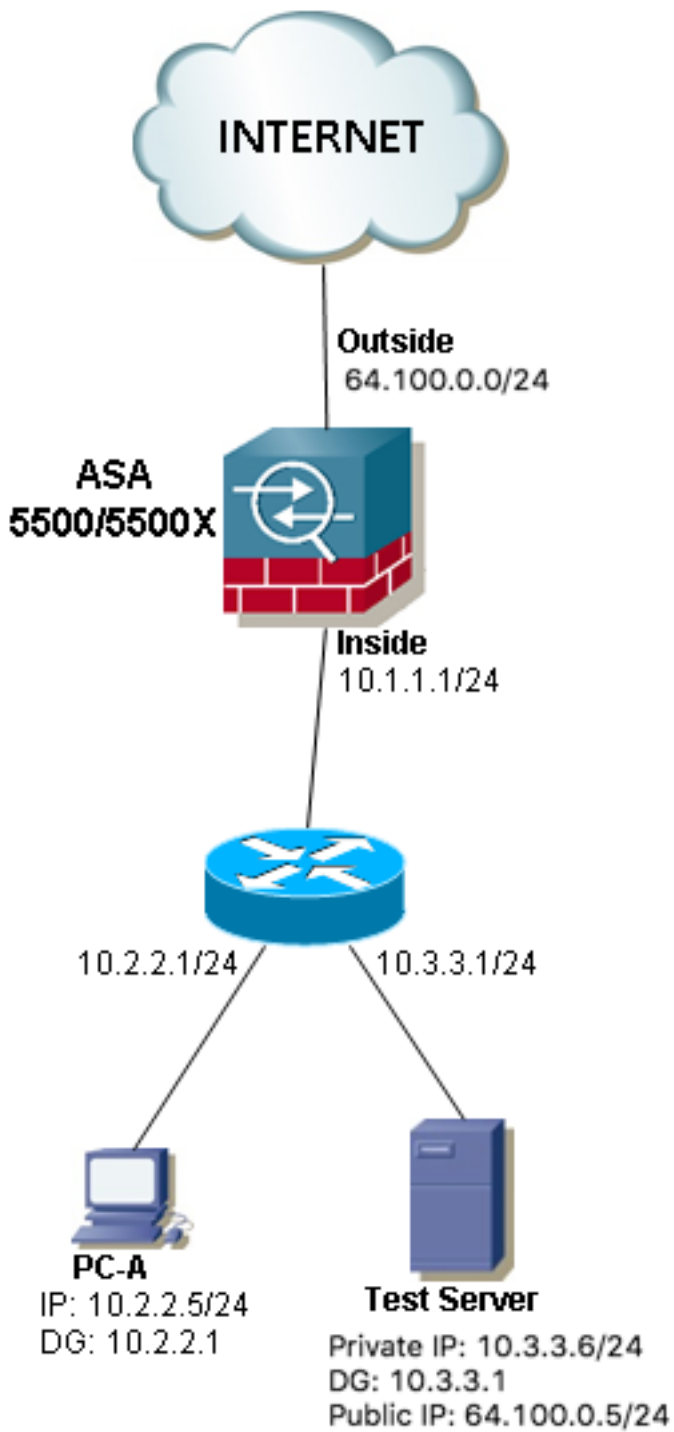
```
ASA# sh cap capin
```

```
10 packets captured
1: 12:50:39.304748 10.1.1.5 > 64.100.0.5: icmp: echo request
2: 12:50:39.335431 64.100.0.5 > 10.1.1.5: icmp: echo reply
3: 12:50:39.368389 10.1.1.5 > 64.100.0.5: icmp: echo request
4: 12:50:39.389368 64.100.0.5 > 10.1.1.5: icmp: echo reply
5: 12:50:39.398432 10.1.1.5 > 64.100.0.5: icmp: echo request
6: 12:50:39.418176 64.100.0.5 > 10.1.1.5: icmp: echo reply
7: 12:50:39.419732 10.1.1.5 > 64.100.0.5: icmp: echo request
8: 12:50:39.425103 64.100.0.5 > 10.1.1.5: icmp: echo reply
9: 12:50:39.434395 10.1.1.5 > 64.100.0.5: icmp: echo request
10: 12:50:39.438423 64.100.0.5 > 10.1.1.5: icmp: echo reply
10 packets shown
```

```
ASA2# sh cap capout
```

```
10 packets captured
1: 12:50:39.305282 10.1.1.1 > 10.1.1.6: icmp: echo request
2: 12:50:39.335386 10.1.1.6 > 10.1.1.1: icmp: echo reply
3: 12:50:39.368663 10.1.1.1 > 10.1.1.6: icmp: echo request
4: 12:50:39.389307 10.1.1.6 > 10.1.1.1: icmp: echo reply
5: 12:50:39.398706 10.1.1.1 > 10.1.1.6: icmp: echo request
6: 12:50:39.418130 10.1.1.6 > 10.1.1.1: icmp: echo reply
7: 12:50:39.419762 10.1.1.1 > 10.1.1.6: icmp: echo request
8: 12:50:39.425072 10.1.1.6 > 10.1.1.1: icmp: echo reply
9: 12:50:39.434669 10.1.1.1 > 10.1.1.6: icmp: echo request
10: 12:50:39.438392 10.1.1.6 > 10.1.1.1: icmp: echo reply
10 packets shown
```

示例3.源主机和目的主机PC-A和测试服务器连接到内部ASA接口，但位于另一第3层设备后面（可以是路由器或多层交换机）。



配置

ASA 8.3及更高版本的两次NAT:

```
object network obj-10.2.2.5
host 10.2.2.5
```

```
object network obj-10.3.3.6
host 10.3.3.6
```

```
object network obj-64.100.0.5
host 64.100.0.5
```

```
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-
```

10.3.3.6

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.

ASA 8.2及更早版本的两次NAT:

```
access-list IN-OUT-INTERFACE extended permit ip host 10.2.2.5 host 64.100.0.5
static (inside,inside) interface access-list IN-OUT-INTERFACE
```

```
access-list OUT-IN-INTERFACE extended permit ip host 10.3.3.6 host 10.1.1.1
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
```

注意: 源IP地址从10.1.1.5转换到ASA内部接口IP地址(10.1.1.1)的NAT转换的主要目的是强制来自主机10.1.1.6的应答返回ASA, 为避免非对称路由并允许ASA, 这是高度必要的要处理感兴趣的主机之间的所有流量, 如果我们不像本例中那样转换源IP地址, 则ASA将因非对称路由而阻止感兴趣的流量。

故障排除

Packet Tracer输出版本8.3及更高版本:

```
ASA# packet-tracer input inside tcp 10.2.2.5 123 64.100.0.5 80
```

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-10.3.3.6
```

Additional Information:

NAT divert to egress interface inside

Untranslate 64.100.0.5/80 to 10.3.3.6/80

Phase: 2

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-10.3.3.6
```

Additional Information:

Static translate 10.2.2.5/123 to 10.1.1.1/123

Phase: 3

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-10.3.3.6
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 167945, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow

Packet Tracer输出版本8.2及更低版本：

```
ASA# packet-tracer input inside tcp 10.2.2.5 123 64.100.0.5 80
```

```
Phase: 1  
Type: UN-NAT  
Subtype: static  
Result: ALLOW  
Config:  
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE  
match ip inside host 10.3.3.6 inside host 10.1.1.1  
static translation to 64.100.0.5  
translate_hits = 0, untranslate_hits = 1
```

Additional Information:

NAT divert to egress interface inside
Untranslate 64.100.0.5/0 to 10.3.3.6/0 using netmask 255.255.255.255

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Phase: 3

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 4

Type: NAT

Subtype:

Result: ALLOW

Config:

```
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.2.2.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
```

Additional Information:

Static translate 10.2.2.5/0 to 10.1.1.1/0 using netmask 255.255.255.255

Phase: 5

Type: NAT

Subtype: host-limits

Result: ALLOW

Config:

```
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.2.2.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
```

Additional Information:

Phase: 6

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.3.3.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
```

Additional Information:

Phase: 7

Type: NAT

Subtype: host-limits

Result: ALLOW

Config:

```
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.3.3.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
```

Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 908, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow

数据包捕获：

```
ASA# sh cap
capture capin type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.2.2.5 host 64.100.0.5
capture capout type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.1 host 10.3.3.6
```

```
ASA# sh cap capin
```

```
10 packets captured
1: 13:06:09.302047 10.2.2.5 > 64.100.0.5: icmp: echo request
2: 13:06:09.315276 64.100.0.5 > 10.2.2.5: icmp: echo reply
3: 13:06:09.342221 10.2.2.5 > 64.100.0.5: icmp: echo request
4: 13:06:09.381266 64.100.0.5 > 10.2.2.5: icmp: echo reply
5: 13:06:09.421227 10.2.2.5 > 64.100.0.5: icmp: echo request
6: 13:06:09.459204 64.100.0.5 > 10.2.2.5: icmp: echo reply
7: 13:06:09.494939 10.2.2.5 > 64.100.0.5: icmp: echo request
8: 13:06:09.534258 64.100.0.5 > 10.2.2.5: icmp: echo reply
9: 13:06:09.564210 10.2.2.5 > 64.100.0.5: icmp: echo request
10: 13:06:09.593261 64.100.0.5 > 10.2.2.5: icmp: echo reply
10 packets shown
```

```
ASA# sh cap capout
```

```
10 packets captured
1: 13:06:09.302367 10.1.1.1 > 10.3.3.6: icmp: echo request
2: 13:06:09.315230 10.3.3.6 > 10.1.1.1: icmp: echo reply
3: 13:06:09.342526 10.1.1.1 > 10.3.3.6: icmp: echo request
4: 13:06:09.381221 10.3.3.6 > 10.1.1.1: icmp: echo reply
5: 13:06:09.421517 10.1.1.1 > 10.3.3.6: icmp: echo request
6: 13:06:09.459174 10.3.3.6 > 10.1.1.1: icmp: echo reply
7: 13:06:09.495244 10.1.1.1 > 10.3.3.6: icmp: echo request
8: 13:06:09.534213 10.3.3.6 > 10.1.1.1: icmp: echo reply
9: 13:06:09.564500 10.1.1.1 > 10.3.3.6: icmp: echo request
10: 13:06:09.593215 10.3.3.6 > 10.1.1.1: icmp: echo reply
10 packets shown
```

相关信息

- [ASA 8.3配置指南：两次NAT的必备条件](#)
- [ASA 8.4配置指南：DNS和NAT](#)
- [ASA 8.3版到8.3版NAT配置示例](#)