基本ASA NAT配置：在DMZ的Web服务器在ASA版本8.3和以上

目录

简介

本文如何提供一简单和直接的示例给configure network地址转换(NAT)和访问控制列表(ACL)在ASA防火墙为了允许出站以及入站连接。本文比运行ASA代码版本9.1(1)写入与一可适应安全工具(ASA) 5510防火墙，但是这能容易地应用到其他ASA防火墙平台。如果使用一个平台例如ASA 5505，使用VLAN而不是物理接口，您需要更改接口类型如适当。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据运行ASA代码版本9.1(1)的ASA 5510防火墙。

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。

概述

目标

在此配置示例中，您能查看什么NAT和ACL配置将是需要的为了提供对一Web服务器的入站访问在ASA防火墙的DMZ，并且允许从内部和DMZ主机的出站连接。这可以汇总作为两个目标：

1. 允许在里面和DMZ出站连接的主机到互联网。
2. 允许在互联网的主机访问在DMZ的一Web服务器用192.168.1.100的IP地址。

在达到必须完成为了实现这两个目标的步骤前，本文在新版本的方式ACL和NAT工作简要地去ASA代码(版本8.3和以上)。

访问控制表概述

访问控制列表(访问列表或ACL简称)是ASA防火墙确定的方法流量是否允许或拒绝。默认情况下，从**更低**通过到**更高安全级别的**流量拒绝。这可以由ACL改写应用对该较低安全性接口。默认情况下，并且ASA允许从更加**高的**流量到**较低安全性接口**。此行为可能也改写与ACL。

在ASA代码中更早版本(8.2和更加早期)， ASA对在接口的ACL比较一流入连接或数据包，无需首先取消转译数据包。换句话说， ACL必须允许数据包，好象您将获取在接口的该数据包。用版本8.3和以上代码，在检查接口ACL前， ASA取消转译该数据包。这为8.3意味着那及以后代码，并且本文，对主机的实时IP的流量允许而不是主机的转换后的IP。

请参阅配置的访问规则图书消毒2 ：思科ASA系列防火墙CLI配置指南， 9.1关于ACL的更多信息。

NAT 概述

在ASA的NAT在版本8.3和以上分成叫作**自动的**两个类型**NAT (对象NAT)**和**手工的NAT (两次NAT)**。第一两个，**对象NAT**，在网络对象定义之内配置。此的示例是提供的以后在本文。此NAT方法一个主要的优点是ASA为处理自动地指令规则为了避免冲突。这是NAT最容易的表，但是与该方便来在配置粒度的一个限制。例如，您不能做出根据在数据包的目的地的转换决策，因为您可能与NAT的第二种类型，**手工nat**。**手工的NAT**是稳健在其粒度，但是要求线路按正确顺序配置，以便能达到正确行为。这复杂化此NAT类型，结果，并且不会用于此配置示例。

请参阅关于NAT图书消毒的信息2 ：思科ASA系列防火墙CLI配置指南， 9.1关于NAT的更多信息。

配置

使用入门

基本ASA配置设置是三个接口连接对三个网段。ISP网段连接对Ethernet0/0接口并且**从外部**标志安全等级0。内部网络连接对Ethernet0/1并且被标记了作为**里面**与安全等级100。DMZ分段， Web服务器驻留，连接对Ethernet0/2并且被标记作为与安全等级的**DMZ** 50。

接口配置和IP地址示例的被看到此处：

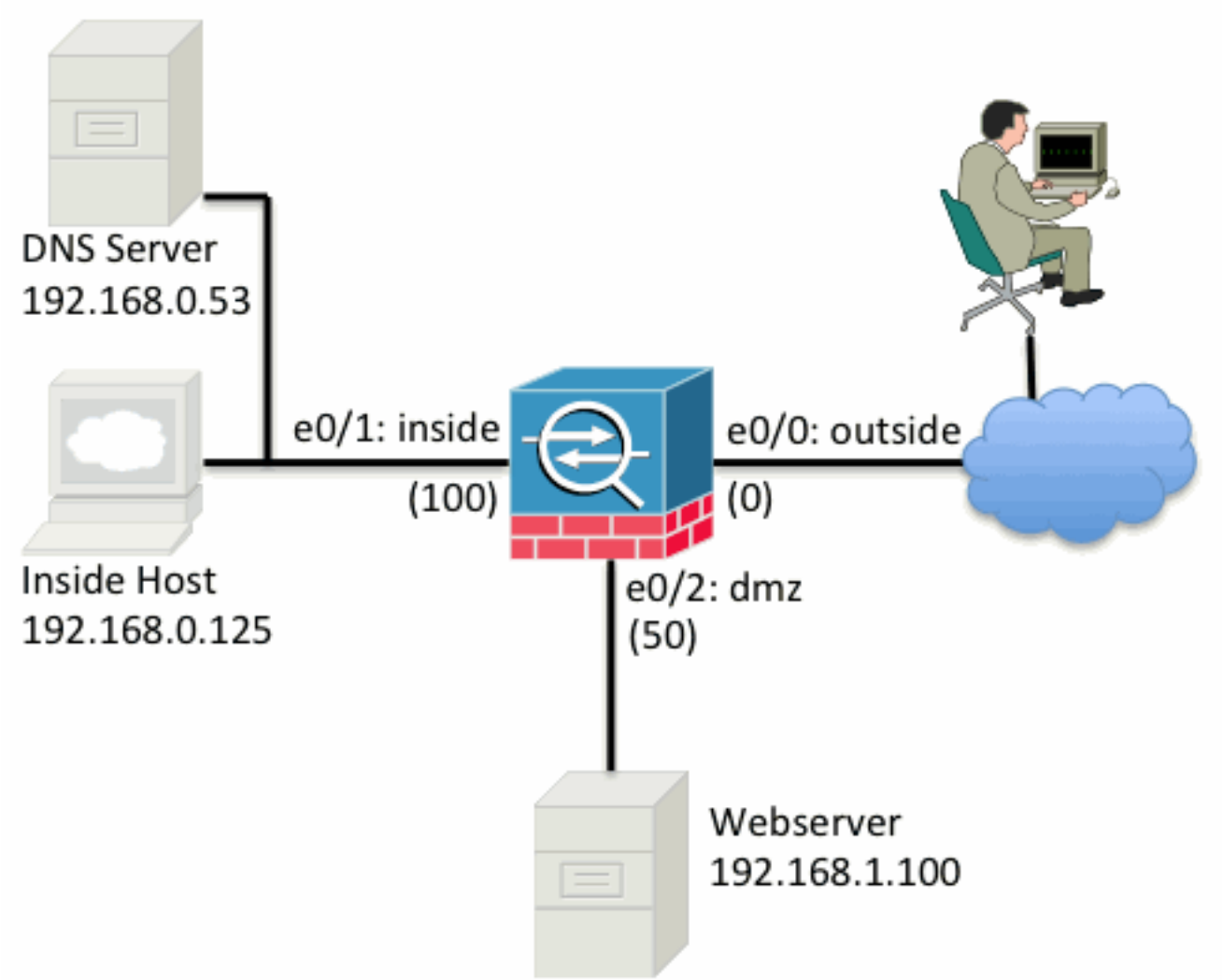
```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
```

```
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

您能看到ASA的**内部接口**设置与192.168.0.1的IP地址，并且它是内部主机的默认网关。ASA的**外部接口**配置与从ISP获取的IP地址。有到位默认路由，设置下一跳是ISP网关。如果使用DHCP自动地提供这。**DMZ**接口配置用192.168.1.1的IP地址，并且它是主机的默认网关在DMZ网段。

拓扑

这是一视觉查看在这如何被缚住并且配置：



Step1 -配置NAT允许主机出去到互联网

对于此示例**对象NAT**，亦称**AutoNAT**，使用。配置的第一件事是允许在**内部的**主机的NAT规则和**DMZ**分段连接对互联网。由于这些主机使用专用IP地址，您需要翻译他们到是可路由的在互联网的事。在这种情况下，请转换地址，以便他们看起来象ASA的**外部接口**IP地址。如果您的外部IP频繁

地更改(或许由于DHCP)这是最直接的方式设置此。

为了配置此NAT，您需要创建表示**里面**子网以及一个表示**DMZ**子网的网络对象。在这些对象中的每一个，请配置端口地址转换(PAT)这些客户端的一个**动态nat**规则，因为他们从他们的各自的接口将通过到**外部接口**。

此配置看似类似于此：

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

如果这时查看运行的配置(与输出**show run命令**)，您看到对象定义拆分到输出的两部分。第一部分只指示什么在对象(主机/子网， IP地址，等等)，而第二部分显示NAT规则附加对该对象。如果在上一个输出中采取首先进入：

*当匹配从**内部接口的**192.168.0.0/24子网横断到**外部接口的**主机，您要动态地翻译他们到**外部接口**。*

步骤2 -配置NAT访问从互联网的Web服务器

即然在**内部**和**DMZ**接口的主机能出去到互联网，您需要修改配置，以便互联网的用户能访问我们的在TCP端口80的Web服务器。在本例中，设置是，以便互联网的人们能连接到ISP提供的另一个IP地址，我们*拥有的*一个另外的IP地址。对于此示例，请使用198.51.100.101。使用此配置，互联网的用户能通过访问在TCP端口80的198.51.100.101到达**DMZ** Web服务器。请使用**对象NAT**此任务，并且ASA Web服务器的(192.168.1.100) translate tcp端口80将看起来象在TCP端口80的198.51.100.101在**外部**。同样于什么以前执行，定义了对象并且定义了该对象的翻译规则。并且，请定义第二个对象代表您将翻译此主机的IP。

此配置看似类似于此：

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

汇总什么该NAT规则在本例中含义：

*当匹配IP地址192.168.1.100在**DMZ**分段的主机建立从**TCP端口**来源的连接**80 (www)**，并且连接出去**外部接口**，您要翻译那是**TCP端口80 (www)**在**外部接口**和翻译该IP地址是**198.51.100.101**。*

那似乎一少许多…“从TCP端口80 (www)来源”，但是Web流量*被注定*到端口80。请注意这些NAT规则是双向本质上。结果，您能翻转字词为了改变措辞此句子。结果更大量有意义：

*当**外部的**主机建立对**198.51.100.101的**连接在目的地TCP**端口80 (www)**，您将翻译目的IP地址是**192.168.1.100**，并且目的地端口将是**TCP端口80 (www)**并且发送它**DMZ**。*

这有更多意义，当措辞这样。其次，您需要设置ACL。

步骤3 -配置ACL

NAT配置，并且此配置结尾近。切记，在ASA的ACL允许您改写如下的默认安全行为：

- 从**较低安全性接口**去的流量**拒绝，**当去**更高安全性接口时**。
- 从**更高安全性接口**去的流量**允许，**当去**较低安全性接口时**。

因此没有所有ACL的新增内容对配置的，在示例的此流量工作：

- 在**里面**(安全等级100)的主机能连接到在**DMZ** (安全等级50)的主机。
- 在**里面**(安全等级100)的主机能连接到在**外部**(安全等级0)的主机。
- 在**DMZ** (安全等级50)的主机能连接到在**外部**(安全等级0)的主机。

然而，此流量拒绝：

- 在**外部**(安全等级0)的主机不能连接到在**里面**(安全等级100)的主机。
- 在**外部**(安全等级0)的主机不能连接到在**DMZ** (安全等级50)的主机。
- 在**DMZ** (安全等级50)的主机不能连接到在**里面**(安全等级100)的主机。

由于流量从自**DMZ**网络的**外面**由与其当前配置的ASA拒绝，互联网的用户不能到达尽管NAT配置的Web服务器在步骤2。您需要明确地允许此流量。用8.3及以后代码您在ACL而不是**转换后的IP**必须使用主机的**雷亚尔德蒙特罗伊IP**。这意味着配置需要允许**而不是**流量被注定对192.168.1.100流量被注定对在端口80的198.51.100.101。For simplicity的缘故，在步骤定义的对象2将使用此ACL。一旦ACL创建，您需要应用它入站在外部接口。

这是什么那些配置命令看上去象：

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

access-list线路状态：

*从**any(where)的**Permit流量到对象**网络服务器**代表的主机**(192.168.1.100)**在端口80。*

是重要配置使用**所有**关键字这里。由于客户端源IP地址没有叫作它到达您的网站，请指定所有含义‘任何IP地址’。

怎么样从**DMZ**分段的流量被注定了对在**网络内部**分段的主机？例如，在**网络内部的**一个服务器在**DMZ**需要的主机连接。ASA如何能准许只特定的流量被注定对**内部的**服务器和块一切别的东西被注定对从**DMZ的里面**分段？

在本例中假设，有在网络内部的一个DNS服务器在**DMZ**需要的主机为DNS解析访问的IP地址192.168.0.53。您创建需要的ACL并且应用它对**DMZ**接口，因此ASA能改写该默认安全行为，前面提到，为进入该接口的流量。

这是什么那些配置命令看上去象：

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

ACL比允许该流量复杂对在UDP端口53的DNS服务器。如果我们的所有是首先‘permit’线路，则所有流量从**DMZ将**阻塞到在互联网的主机。ACL有隐式‘deny ip any any’在ACL结束时。结果，您的**DMZ**主机不能出去到互联网。默认情况下即使从**DMZ的**流量到**外部**允许，与ACL的应用程序对

DMZ接口的，那些默认DMZ接口的安全行为实际上不再是，并且您必须明确地允许在接口ACL的流量。

步骤4 -与数据包跟踪程序功能的测验配置

即然配置完成，您需要测试它为了确保它工作。(如果这是您的网络)，最容易的方法将使用实际主机。然而，为了测试此从CLI和更加进一步测试某些ASA的工具，请使用数据包跟踪程序为了测试和潜在调试遇到的所有问题。

数据包跟踪程序工作在模拟根据一系列的参数的数据包旁边，并且注入该数据包对接口数据路径，类似于一真实生活数据包会的方式，如果被拾起电线。此数据包通过完成检查和进程的无数被跟随，当穿过防火墙，并且数据包跟踪程序注释结果。模拟出去对在互联网的一台主机的内部主机。下面的命令提示防火墙对：

*模拟来自在**内部接口的TCP数据包**在源端口**12345的**IP地址**192.168.0.125**被注定对**203.0.113.1的**IP地址在端口**80的**。*

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

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: per-session
```

```
Result: ALLOW
Config:
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 1, packet dispatched to next module

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

最终结果**从外部**是流量**允许**，通过所有NAT和ACL登记配置和被派出出口接口的whichmeans。注意数据包在相位3翻译，并且该相位详细信息显示什么规则点击。主机192.168.0.125动态地翻译对198.51.100.100根据配置。

现在，为一连接请运行它从互联网到Web服务器。切记，在互联网的主机将通过连接访问Web服务器对在**外部接口的**198.51.100.101。再次，此下一条命令翻译对：

*模拟来自在**外部接口的TCP数据包**在源端口**12345的**IP地址**192.0.2.123**被注定对**198.51.100.101的**IP地址在端口**80的**。*

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
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 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

再次，结果是数据包允许。ACL优良检查，配置查找，并且互联网的用户(**从外部**)应该能访问有外部IP的该Web服务器。

验证

验证程序在步骤4包括-测试与数据包跟踪程序功能的配置。

故障排除

目前没有针对此配置的故障排除信息。

结论

要执行基本NAT的ASA的配置不是那威吓任务。如果更换用于配置示例，和端口的IP地址在本文的示例可以适应您的特定方案。此的最终ASA配置，当结合，为ASA 5510查找类似于此：

```
ASA Version 9.1(1)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

在当接口的ASA 5505，例如，连接如以前显示(**外部**连接自Ethernet0/0，**在**已连接对Ethernet0/1和**DMZ里面**连接对Ethernet0/2)：

```
ASA Version 9.1(1)
!
interface Ethernet0/0
description Connected to Outside Segment
switchport access vlan 2
!
interface Ethernet0/1
description Connected to Inside Segment
switchport access vlan 1
```

```
!
interface Ethernet0/2
description Connected to DMZ Segment
switchport access vlan 3
!
interface Vlan2
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```