Основная конфигурация NAT ASA: Web-сервер в DMZ в версии ASA 8.3 и позже

Содержание

Введение

Этот документ предоставляет простой и прямой пример того, как настроить сетевую Переадресацию (NAT) и Списки контроля доступа (ACL) на Межсетевом экране ASA для разрешения исходящего, а также входящего подключения. Этот документ был записан с Устройством адаптивной защиты (ASA) 5510 межсетевых экранов, чем версия кода 9.1 (1) ASA выполнений, но это может легко примениться к любой другой платформе межсетевого экрана ASA. При использовании платформу, такую как ASA 5505, который использует VLAN вместо физического интерфейса, необходимо изменить типы интерфейса как соответствующие.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на межсетевом экране ASA 5510, который

выполняет версию кода 9.1 (1) ASA.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Обзор

Цели

В конфигурации данного примера можно посмотреть на то, что будут необходимы NAT и конфигурация списков управления доступом (ACL), чтобы позволить входящий доступ Web-серверу в DMZ межсетевого экрана ASA и позволить исходящее подключение от хостов DMZ и внутреннего. Это может быть суммировано как две цели:

1. Позвольте хосты на внутренней части и DMZ исходящее подключение к Интернету.
2. Позвольте хостам в Интернете обращаться к Web-серверу на DMZ с IP-адресом 192.168.1.100.

Прежде, чем добраться до шагов, которые должны быть выполнены для выполнения этих двух целей, этот документ кратко пробегается через способ, которым ACL и NAT работают на более новые версии кода ASA (версия 8.3 и позже).

Обзор списка контроля доступа

Списки контроля доступа (Access-lists или ACL, если коротко) являются методом, которым межсетевой экран ASA определяет, разрешен ли трафик или запрещен. По умолчанию трафик, который проходит от **более низкого** до **высшего уровня безопасности**, запрещен. Это может быть отвергнуто ACL, применился к тому интерфейсу с более низким уровнем безопасности. Также ASA, по умолчанию, позволяет трафик от **выше** до **интерфейсов с более низким уровнем безопасности**. Это поведение может также быть отвергнуто с ACL.

В более ранних версиях кода ASA (8.2 и ранее), ASA сравнил входящее соединение или пакет против ACL на интерфейсе, не не преобразовывая пакет сначала. Другими словами, ACL должен был разрешить пакет, как будто необходимо было перехватить тот пакет на интерфейсе. В версии 8.3 и коде следующих версий, ASA не преобразовывает тот пакет, прежде чем это проверит интерфейсные ACL. Это означает, что для 8.3 и код следующих версий и этот документ, трафик к реальному IP хоста разрешен а не преобразованный IP хоста.

Посмотрите раздел Правил Доступа Настройки Книги 2: Руководство Конфигурации интерфейса командой строки Межсетевого экрана Серии Cisco ASA, 9.1 для получения дополнительной информации о ACL.

Обзор NAT

NAT на ASA в версии 8.3 и позже разделен на два типа, известные как **Автоматический NAT (Объект NAT)** и **Руководство NAT (Дважды NAT)**. Первый из этих двух, **Объект NAT**, настроен в рамках определения сетевого объекта. Пример этого предоставлен позже в этом документе. Одно основное преимущество этого метода NAT состоит в том, что ASA

автоматически упорядочивает правила для обработки во избежание конфликтов. Это - самая легкая форма NAT, но с той простотой прибывает ограничение в глубину детализации конфигурации. Например, вы не можете принять решение трансляции на основе назначения в пакете, как вы могли со вторым типом NAT, **Ручного Nat**. **Ручной NAT** более устойчив в своей глубине детализации, но он требует, чтобы линии были настроены в правильном порядке так, чтобы он мог достигнуть правильного поведения. Это усложняет этот тип NAT, и в результате он не будет использоваться в этом примере конфигурации.

Посмотрите информацию О разделе NAT Книги 2: Руководство Конфигурации интерфейса командой строки Межсетевого экрана Серии Cisco ASA, 9.1 для получения дополнительной информации о NAT.

Настройка

Начать работу

Основная настройка конфигурации ASA является тремя интерфейсами, связанными с тремя сегментами сети. Сегмент сети ISP связан с интерфейсом Ethernet0/0 и маркирован **снаружи** с уровнем безопасности 0. Внутренняя сеть была связана с Ethernet0/1 и маркирована как **внутри** с уровнем безопасности 100. Сегмент DMZ, где Web-сервер находится, связан с Ethernet0/2 и маркирован как **DMZ** с уровнем безопасности 50.

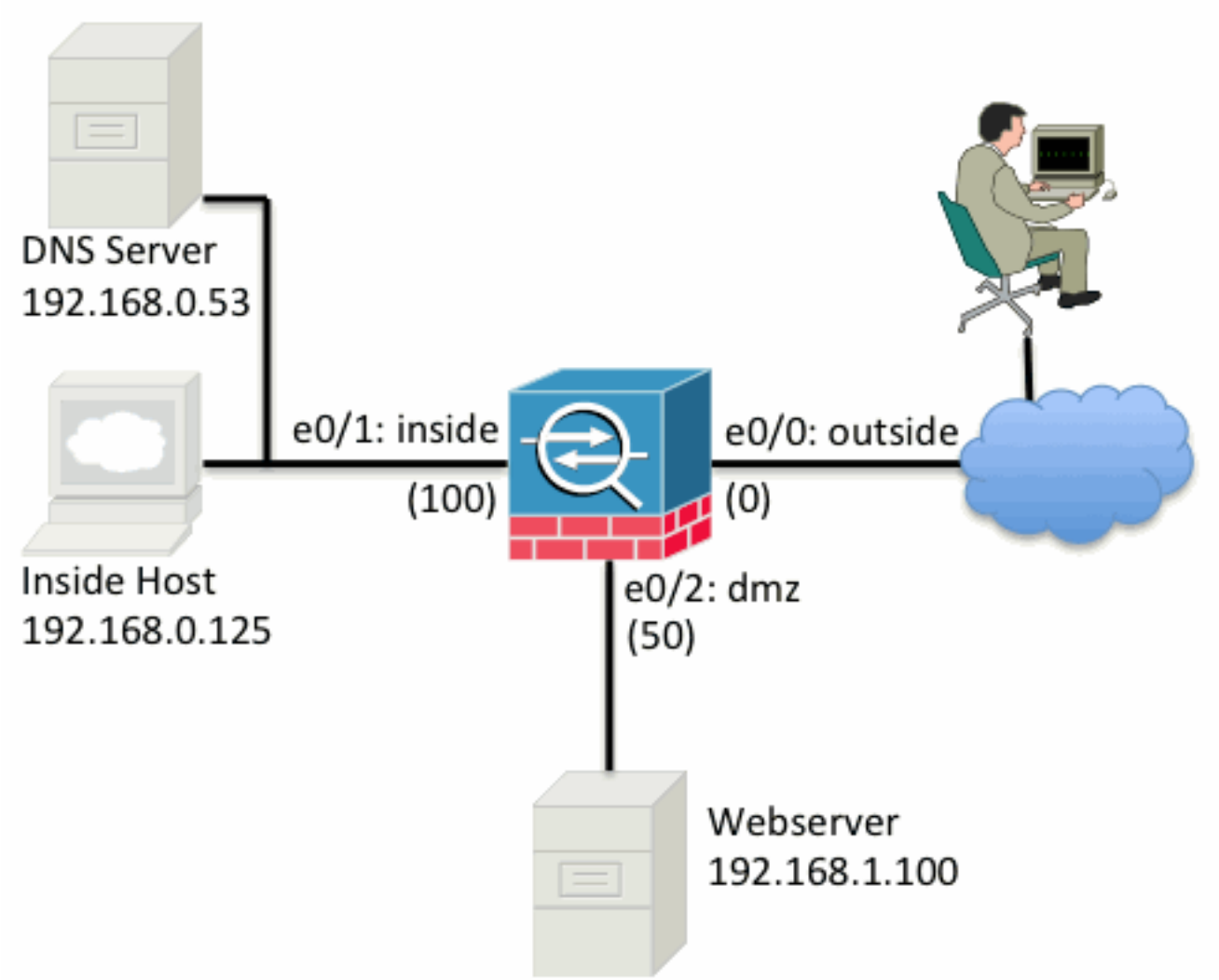
Конфигурация интерфейса и IP-адреса для примера замечены здесь:

```
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
```

Здесь вы видите, что **Внутренний интерфейс ASA** установлен с IP-адресом 192.168.0.1, и это - шлюз по умолчанию для внутренних хостов. **Внешний интерфейс** ASA настроен с IP-адресом, полученным из интернет-провайдера. Там существует маршрут по умолчанию, который заставляет следующий переход быть шлюзом поставщика. При использовании DHCP, это предоставлено автоматически. Интерфейс **DMZ** настроен с IP-адресом 192.168.1.1, и это - шлюз по умолчанию для хостов на сегменте сети DMZ.

Топология

Вот визуальный взгляд на то, как это телеграфировано и настроено:



Шаг 1 - настраивает NAT, чтобы позволить хостам выходить в Интернет

Для **Объекта** данного примера **NAT**, также известный как **AutoNAT**, используется. Первой вещью настроить являются правила NAT, которые позволяют хостам на **внутренней части** и сегментах **DMZ** соединяться с Интернетом. Поскольку эти хосты используют закрытые IP - адреса, необходимо преобразовать их во что-то, что маршрутизируемо в Интернете. В этом случае преобразуйте адреса так, чтобы они были похожи на IP-адрес **внешнего интерфейса** ASA. Если ваш внешний IP часто изменяется (возможно, из-за DHCP), это - самый прямой способ настроить это.

Для настройки этого NAT необходимо создать сетевой объект, который представляет **внутреннюю** подсеть, а также ту, которая представляет **подсеть DMZ**. В каждом из этих объектов настройте **правило динамического преобразования сетевых адресов (NAT)**, которое будет Преобразование адресов портов (PAT) эти клиенты, поскольку они проходят от их соответствующих интерфейсов до **внешнего интерфейса**.

Эта конфигурация выглядит подобной этому:

```
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
```

При рассмотрении рабочей конфигурации на этом этапе (с выходными данными **команды show run**), вы будете видеть, что определение объекта разделено на две части выходных данных. Первая часть только указывает на то, что находится в объекте (хост/подсеть, IP-адрес, и так далее), в то время как второй раздел показывает, что правило NAT связало с тем объектом. Если вы берете первую запись в предыдущих выходных данных:

*Когда хосты, которые совпадают с 192.168.0.0/24 пересечением подсети от **внутреннего интерфейса** до **внешнего интерфейса**, вы хотите динамично преобразовать их во **внешний интерфейс**.*

Шаг 2 - настраивает NAT для доступа к Web-серверу из Интернета

Теперь, когда хосты на **внутренней части** и интерфейсах **DMZ** могут выйти к Интернету, необходимо модифицировать конфигурацию так, чтобы пользователи в Интернете могли обратиться к нашему Web-серверу на порте TCP 80. В данном примере настройка состоит в том так, чтобы люди в Интернете могли подключить с другим IP-адресом интернет-провайдера, если, дополнительный IP-адрес мы *владеем*. Для данного примера используйте 198.51.100.101. С этой конфигурацией пользователи в Интернете будут в состоянии достигнуть Web-сервера **DMZ** путем доступа 198.51.100.101 на порте TCP 80. Используйте **Объект NAT** для этой задачи, и ASA будет порт 80 translate TCP на Web-сервере (192.168.1.100) для сходства с 198.51.100.101 на порте TCP 80 на **внешней стороне**. Так же к тому, что было сделано ранее, определите объект и определите правила трансляции для того объекта. Кроме того, определите второй объект для представления IP, которого вы преобразуете этот хост.

Эта конфигурация выглядит подобной этому:

```
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
```

Только для суммирования что, который правило NAT означает в данном примере:

*Когда хост, который совпадает с IP-адресом **192.168.1.100** на сегментах **DMZ**, устанавливает соединение, полученное от **порта TCP 80 (www)** , и то соединение выходит **внешний интерфейс**, вы хотите преобразовать это, чтобы быть **портом TCP 80 (www)** на **внешнем интерфейсе** и преобразовать тот IP-адрес, чтобы быть **198.51.100.101**.*

Это кажется немного нечетным... "полученный от порта TCP 80 (www)", но веб - трафик *предназначен* к порту 80. Важно понять, что эти правила NAT являются двунаправленными по своей природе. В результате можно зеркально отразить формулировку вокруг для перефразирования этого предложения. Результат имеет намного больше смысла:

*Когда хосты на **внешней стороне** установят соединение с **198.51.100.101** на **порту 80 TCP - получателя (www)**, вы преобразуете IP - адрес назначения, чтобы быть **192.168.1.100**, и порт назначения будет **портом TCP 80 (www)** и передаст ему **DMZ**.*

Это имеет больше смысла, когда формулируется этот путь. Затем, необходимо установить ACL.

Шаг 3 - настраивает ACL

NAT настроен, и конец этой конфигурации рядом. Помните, ACL на ASA позволяют вам отвергать безопасное поведение по умолчанию, которое является следующие:

- Трафик, который идет от **интерфейса с более низким уровнем безопасности, запрещен**, когда он переходит **к интерфейсу с более высоким уровнем безопасности**.
- Трафик, который идет от **интерфейса с более высоким уровнем безопасности, позволен**, когда он переходит **к интерфейсу с более низким уровнем безопасности**.

Таким образом без добавления любых ACL к конфигурации, этот трафик в примере работает:

- Хосты на **внутренней части** (уровень безопасности 100) могут соединиться с хостами на **DMZ** (уровень безопасности 50).
- Хосты на **внутренней части** (уровень безопасности 100) могут соединиться с хостами на **внешней стороне** (уровень безопасности 0).
- Хосты на **DMZ** (уровень безопасности 50) могут соединиться с хостами на **внешней стороне** (уровень безопасности 0).

Однако этот трафик запрещен:

- Хосты на **внешней стороне** (уровень безопасности 0) не могут соединиться с хостами на **внутренней части** (уровень безопасности 100).
- Хосты на **внешней стороне** (уровень безопасности 0) не могут соединиться с хостами на **DMZ** (уровень безопасности 50).
- Хосты на **DMZ** (уровень безопасности 50) не могут соединиться с хостами на **внутренней части** (уровень безопасности 100).

Поскольку трафик от **внешней стороны** до **сети DMZ** запрещен ASA с его текущей конфигурацией, пользователи в Интернете не могут достигнуть Web-сервера несмотря на конфигурацию NAT в шаге 2. Необходимо явно разрешить этот трафик. В 8.3 и код следующих версий необходимо использовать **Реального IP** хоста в ACL а не **преобразованного IP**. Это означает потребности конфигурации разрешить трафик, предназначенный к 192.168.1.100 и **НЕ** трафик, предназначенный к 198.51.100.101 на порту 80. Для пользы простоты объекты, определенные в шаге 2, будут использоваться для этого ACL также. Как только ACL создан, необходимо применить его входящий на внешний интерфейс.

Вот то, на что похожи те команды настройки:

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

Состояния линии access-list:

*Трафик разрешения от **любого** (где) к хосту, представленному объектным **веб-сервером (192.168.1.100)** на порту 80.*

Важно, чтобы конфигурация использовала **любое** ключевое слово здесь. Поскольку IP - адрес источника клиентов не известен, поскольку он достигает вашего веб-сайта, задайте любое значение 'Любой IP-адрес'.

Что относительно трафика от сегмента **DMZ**, предназначенного к хостам на сегменте **внутренней сети**? Например, сервер на **внутренней сети**, с которой должны соединиться хосты на **DMZ**. Как ASA может позволить только, что определенный трафик,

предназначенный к **внутреннему** серверу и, блокирует все остальное предназначенное к **внутреннему** сегменту от **DMZ**?

В данном примере предполагается, что существует сервер DNS на внутренней сети в IP-адресе 192.168.0.53, к которому хосты на **DMZ** должны обратиться для Разрешения DNS. Вы создаете необходимый ACL и применяете его к интерфейсу **DMZ**, таким образом, ASA может отвергнуть то безопасное поведение по умолчанию, упомянутое ранее, для трафика, который вводит тот интерфейс.

Вот то, на что похожи те команды настройки:

```
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 более сложен, чем простое разрешение что трафик к серверу DNS на порту 53 UDP. Если все, что мы сделали, - то, которые сначала 'разрешают' линию, то весь трафик был бы заблокирован от **DMZ** до хостов в Интернете. ACL имеют неявное, 'deny ip any any' в конце ACL. В результате ваши хосты **DMZ** не были бы в состоянии выйти в Интернет. Даже при том, что трафик от **DMZ** до **внешней стороны** разрешен по умолчанию с приложением ACL к интерфейсу **DMZ**, то безопасное поведение по умолчанию для интерфейса **DMZ** больше не в действительности, и необходимо явно разрешить трафик в интерфейсном ACL.

Шаг 4 - тестирует конфигурацию с пакетной функцией трассировщика

Теперь, когда конфигурация завершена, необходимо протестировать ее, чтобы удостовериться, что она работает. Наилегчайший метод должен использовать фактические хосты (если это - ваша сеть). Однако в интересах тестирования этого от CLI и дальнейшего исследования некоторых программных средств ASA, используйте пакетный трассировщик, чтобы протестировать и потенциально отладить любые проблемы, с которыми встречаются.

Пакетный трассировщик работает путем моделирования пакета на основе серии параметров и введения того пакета к интерфейсному каналу передачи данных, подобному способу, которым был бы реальный пакет, если это было взято от провода. Этот пакет придерживается через несметное число проверок и процессов, которые сделаны, поскольку это проходит через межсетевой экран, и пакетный трассировщик обращает внимание на результат. Моделируйте внутренний хост, выходящий в хост в Интернете. Команда ниже сообщает межсетевому экрану к:

*Моделируйте **пакет TCP**, прибывающий во **внутренний интерфейс** от IP-адреса **192.168.0.125** на исходном порте **12345** предназначенных к IP-адресу **203.0.113.1** на **порту 80**.*

```
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
```

Конечный результат - то, что трафик **позволен**, whichmeans, что он передал весь NAT, и ACL

регистрируется в конфигурации и был отослан исходящий интерфейс, **снаружи**. Обратите внимание на то, что пакет был преобразован в фазе 3 и подробных данных того Фазового показа, какое правило поражено. Хост 192.168.0.125 преобразован динамично в 198.51.100.100 согласно конфигурации.

Теперь, выполните его для соединения от Интернета до Web-сервера. Помните, хосты в Интернете обратятся к Web-серверу путем соединения с 198.51.100.101 на **внешнем интерфейсе**. Снова, эта следующая команда преобразовывает в:

*Моделируйте **пакет TCP**, прибывающий во **внешний интерфейс** от IP-адреса **192.0.2.123** на исходном порте **12345** предназначенных к IP-адресу **198.51.100.101** на **порту 80**.*

```
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
```

Снова, результат состоит в том, что позволен пакет. Выезд ACL, конфигурация выглядит хорошо, и пользователи в Интернете **(снаружи)** должны быть в состоянии обратиться к тому Web-серверу с внешним IP.

Проверка

Процедуры проверки включены в Шаг 4 - Тестирование Конфигурации с Пакетной Функцией Трассировщика.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Заключение

Конфигурация ASA, чтобы сделать основной NAT не то, что укрощение задачи. Пример в этом документе может быть адаптирован к вашему определенному сценарию при изменении IP-адресов и портов, используемых в примерах конфигурации. Заключительная конфигурация ASA для этого, когда объединено, выглядит подобной этому для ASA 5510:

```
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
```

На ASA 5505, например, с интерфейсами, связанными как показано ранее (**снаружи** связанный с Ethernet0/0, **внутри** связанным с Ethernet0/1 и **DMZ** , связанным с 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
```