PIX/ASA 7.X : Включение/отключение связи между интерфейсами

Содержание

Введение

В этом документе представлен пример конфигурации для различных типов соединений между интерфейсами устройства безопасности ASA/PIX.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- IP-адреса и присвоение шлюза по умолчанию
- Подключение физической сети между устройствами
- Номер коммуникационного порта задан для реализованной услуги

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Модули ASA под управлением ПО версии 7.x или выше
- Windows 2003 Server
- Рабочие станции Windows XP

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.

Родственные продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения:

- Межсетевые экраны PIX 500, которые работают 7.x и позже

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В этом документе описываются действия, необходимые для обеспечения обмена данными между интерфейсами. Обсуждены формы общения, такие как они:

1. Соединения от хостов, расположенных во внешней сети и пытающихся получить доступ к ресурсам в DMZ
2. Соединения от хостов, расположенных во внутренней сети и пытающихся получить доступ к ресурсам в DMZ
3. Соединения от хостов, расположенных во внутренней сети и пытающихся получить доступ к ресурсам во внешней сети

NAT

В нашей конфигурации используется преобразование сетевых адресов (NAT) и преобразование адресов портов (PAT). Преобразование заменяет фактический (локальный) адрес пакета назначенным (глобальным) адресом, который маршрутизируется во внешнюю сеть. Преобразование NAT состоит из двух этапов: процесс преобразования фактического адреса в назначенный адрес и процесс обратного преобразования ответного трафика. Существует два типа преобразования адресов, которые будут использоваться в этом руководстве: статическое и динамическое.

Динамическое преобразование позволяет каждому хосту использовать разные адреса или порты для каждого последующего преобразования. Динамическое преобразование можно

использовать, когда локальные хосты используют один или несколько общих глобальных адресов (т.е. скрываются за ними). В этом режиме локальный адрес не может зарезервировать глобальный адрес для преобразования. Вместо этого преобразование адресов выполняется по принципу "многие к одному" или "многие ко многим". Записи преобразования создаются только при необходимости. Как только использование записи преобразования прекращается, запись удаляется и становится доступна другим локальным хостам. Этот тип преобразования наиболее полезен для исходящих соединений, в которых хостам назначается динамический адрес и номер порта только при создании соединений. Существует два типа динамического преобразования адресов:

- Динамическое преобразование NAT — локальные адреса преобразуются в следующий доступный глобальный адрес. Преобразование выполняется по принципу один к одному, поэтому существует вероятность нехватки адресов в пуле, если большое число локальных хостов запросят преобразование одновременно.
- Перегрузка NAT (PAT) — локальные адреса преобразуются в один глобальный адрес. Уникальные соединения создаются, когда старший номер порта глобального адреса назначается источником соединения. Преобразование выполняется по принципу "многие к одному", так как хосты используют один общий глобальный адрес.

Статическое преобразование создает фиксированное преобразование фактического адреса или адресов в назначенный адрес или адреса. Статическая конфигурация NAT назначает один адрес каждому соединению и является постоянным правилом преобразования. Статическое преобразование используется, когда внутренний или локальный хост должен иметь одинаковый глобальный адрес при каждом соединении. Преобразование адресов выполняется по принципу "один к одному". Статическое преобразование можно задать для одного хоста или для всех адресов в IP-подсети.

Главное различие между динамическим преобразованием NAT и диапазоном адресов для статического преобразования NAT заключается в том, что статическое преобразование NAT позволяет удаленному хосту инициировать соединение с преобразуемым хостом (если список доступа разрешает это), в то время как динамическое преобразование NAT не позволяет этого. Кроме того, для статического преобразование NAT необходимо количество назначенных адресов, равное количеству внутренних адресов.

Устройство безопасности преобразует адрес, если трафик соответствует правилу NAT. Если никакое правило NAT не совпадает, обрабатывание для пакета продолжается. Исключение имеет место, когда контроль NAT включен. Контроль NAT требует, чтобы пакеты, которые передаются с более безопасного (внутреннего) на менее безопасный (внешний) интерфейс, должны соответствовать правилу NAT, в противном случае обработка пакета прекращается. Общие сведения о конфигурации см. в документе PIX/ASA 7.x NAT и PAT . Подробные сведения о принципе работы NAT см. в документе Принцип работы NAT.

Совет: При изменении конфигурации NAT рекомендуется удалить текущие преобразования NAT. **Таблицу преобразования NAT можно очистить с помощью команды clear xlate. Однако возьмите внимание, когда вы делаете это** начиная с очистки таблицы преобразования разъединяет все текущие соединения то использование трансляции. Можно избежать очистки таблицы преобразования, подождав истечения времени ожидания текущих записей преобразования, но это не рекомендуется, поскольку непредвиденные операции могут привести к созданию новых соединений на основе новых правил.

Уровни безопасности

Значение уровня безопасности определяет, как хосты и устройства, подключенные к разным интерфейсам, взаимодействуют друг с другом. По умолчанию хосты/устройства, связанные с интерфейсами с высшими уровнями безопасности, могут обратиться к хостам/устройствам, связанным с интерфейсом с низкими уровнями безопасности. Хосты и устройства, подключенные к интерфейсу с более низким уровнем безопасности не могут получать доступ к хостам и устройствам, подключенным к интерфейсу с более высоким уровнем безопасности без соответствующего разрешения в списке доступа.

Команда security-level является новой в версии 7.0 и заменяет часть команды nameif, которая служит для назначения уровня безопасности интерфейсу. Два интерфейса, "внутренний" и "внешний", имеют уровни безопасности по умолчанию, но их можно переопределить с помощью команды security-level. При именовании интерфейса "внутри" ему дают уровень безопасности по умолчанию 100; интерфейс, названный "снаружи", дан уровень безопасности по умолчанию 0. Все другие недавно добавленные интерфейсы получают уровень безопасности по умолчанию 0. **Чтобы назначить интерфейсу новый уровень безопасности, используйте команду security-level в режиме команд интерфейса.** Уровни безопасности колеблются от 1-100.

Примечание: Уровни безопасности используются только чтобы определить,как сетевой экранинспектирует и обрабатывает трафик. Например к трафику, передаваемому с более безопасного интерфейса на менее безопасный, по умолчанию применяются менее строгие политики безопасности, чем к трафику, который передается с менее безопасного интерфейса на более безопасный. Для получения дополнительной информации об уровнях безопасности обратитесь к ASA/PIX 7.x Справочник по командам.

ASA/PIX 7.x также представил способность настроить несколько интерфейсов с тем же уровнем безопасности. Например группе интерфейсов, подключенным к сетям партнеров и другим DMZ, можно назначить уровень безопасности 50. По умолчанию эти интерфейсы с одинаковым уровнем безопасности не могут взаимодействовать друг с другом. **Чтобы обойти это ограничение была добавлена команда same-security-traffic permit, которая действует на все интерфейсы**. Эта команда обеспечивает связь между интерфейсами того же уровня безопасности. Дополнительные сведения о взаимодействии интерфейсов с одинаковым уровнем безопасности см. в разделе Настройка параметров интерфейса справочного руководства по командам. Кроме того, ознакомьтесь с этим примером.

ACL

Списки контроля доступа, как правило, состоят из нескольких записей контроля доступа (ACE), которые устройство безопасности упорядочивает в связный список. ACE описывает тип трафика, например с хоста или сети, и перечисляет действия, применимые к данному трафику, обычно разрешающего или отклоняющего характера. Если пакет подпадает под действие списка контроля доступа, устройство безопасности Cisco в своем связном списке ищет ACE, соответствующие пакету. **К пакету применяется первая запись ACE, найденная устройством безопасности.** После того, как соответствующая запись ACE будет найдена, указанное в ней действие (разрешить или отклонить) применяется к пакету.

На интерфейсах можно задавать по одному списку доступа на каждое направление. Это значит, что на интерфейсе можно задать только один список доступа для входящего трафика и один список доступа для исходящего трафика. Списки доступа, которые не применены к интерфейсам, таким как ACL NAT, неограниченны.

Примечание: По умолчанию, весь access-lists имеют неявный ACE в конце, который

запрещает весь трафик, таким образом, весь трафик, который не совпадает ни с каким ACE, который вы вводите в список доступа, совпадает, неявные запрещают в конце, и отброшен. Чтобы трафик мог проходить через интерфейс, в списке доступа необходимо задать хотя бы одну разрешающую инструкцию. Без разрешающей инструкции весь трафик будет отклоняться.

Примечание: Список доступа внедрен с **командами access-list и access-group**. **Эти команды используются вместо команд conduit и outbound, которые применялись в предыдущих версиях ПО для сетевых экранов PIX.** Дополнительные сведения о списках контроля доступа см. в документе Настройка списка доступа по протоколу IP.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В этом документе используется следующая конфигурация сети:

Начальная конфигурация

Эти конфигурации используются в данном документе:

- В этой базовой конфигурации сетевого экрана нет инструкций NAT/STATIC.
- Нет никаких примененных ACL, таким образом, в настоящее время используется неявный ACE `deny any any`.

Имя устройства 1

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif Outside security-level 0 ip
address 172.22.1.163 255.255.255.0 ! interface
Ethernet0/1 nameif inside security-level 100 ip address
172.20.1.1 255.255.255.0 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 192.168.1.1
255.255.255.0 ! interface Ethernet0/3 nameif DMZ-2-
testing security-level 50 ip address 192.168.10.1
255.255.255.0 ! interface Management0/0 shutdown no
nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name corp.com pager lines 24 mtu
inside 1500 mtu Outside 1500 mtu DMZ 1500 no failover
icmp unreachable rate-limit 1 burst-size 1 no asdm
history enable arp timeout 14400 nat-control route
Outside 0.0.0.0 0.0.0.0 172.22.1.1 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 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
preset_dns_map parameters 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 netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

DMZ к внутренней части

Для разрешения связи с DMZ на узлы внутренней сети используйте эти команды. В данном примере Web-сервер на DMZ должен обратиться к AD и серверу DNS на внутренней части.

1. Создайте статическую запись NAT для сервера AD/DNS в DMZ. Статическая запись NAT создает фиксированное преобразование фактического адреса в назначенный адрес. Этот сопоставленный адрес является адресом, который хосты DMZ могут использовать для доступа к серверу на внутренней части без потребности знать действительный адрес сервера. Эта команда сопоставляет адрес DMZ 192.168.2.20 с реальным внутренним адресом 172.20.1.5.`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. Списки контроля доступа должны разрешать интерфейсам с более высоким уровнем безопасности получать доступ к интерфейсам с более низким уровнем безопасности. В данном примере мы даем Web-сервер, который находится на DMZ (Безопасность 50) доступ к AD/серверу DNS на внутренней части (Безопасность 100) с этими определенными сервисными портами: DNS, Kerberos и LDAP.`ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq domainASA-AIP-CLI(config)# access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq 389`**Примечание:** ACL разрешают доступ к сопоставленному адресу AD/сервера DNS, который был создан в данном примере а не реальном внутреннем адресе.
3. В этом шаге вы применяете ACL к интерфейсу DMZ во входящем направлении с этой командой:`ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ`**Примечание:** Чтобы отключить или заблокировать порт 88, например, трафик из DMZ во внутреннюю сеть используйте следующую команду:`ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88`**Совет:** При изменении конфигурации NAT рекомендуется удалить текущие преобразования NAT. **Таблицу преобразования NAT можно очистить с помощью команды clear xlate. Но будьте осторожны при выполнении этой операции, поскольку очистка таблицы преобразования приведет к разрыву всех текущих подключений, использующих записи преобразования.** Альтернатива очистке таблицы преобразования должна ждать текущих преобразований для таймаута, но это не рекомендуется, потому что неожиданное поведение может закончиться, поскольку новые соединения созданы с новыми правилами.Другие распространенные конфигурации:Почтовые серверы в DMZДоступ SSH внутри и снаружиРазрешенные

[сеансы удаленного рабочего стола через устройства PIX/ASA](#)[Другие решения DNS, используемые в DMZ](#)

Интернет — DMZ

Чтобы разрешить подключение пользователей через Интернет и внешние интерфейсы (уровень безопасности 0) к веб-северу в DMZ (уровень безопасности 50), используйте следующие команды:

1. Создайте статическое преобразование для веб-сервера в DMZ во внешнюю сеть. Статическая запись NAT создает фиксированное преобразование фактического адреса в назначенный адрес. Этот назначенный адрес используются хостами в Интернете для доступа к веб-серверу во внутренней сети без необходимости в фактическом адресе сервера. Эта команда привязывает адрес внешнего интерфейса 172.22.1.25 к фактическому адресу DMZ 192.168.1.10.`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. Создайте список контроля доступа, разрешающий пользователям внешней сети получать доступ к веб-серверу через назначенный адрес. Обратите внимание, что на веб-сервере также работает FTP-сервер.`ASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`
3. Последний этап настройки — применение списка контроля доступа к внешнему интерфейсу для входящего трафика.`ASA-AIP-CLI(config)# access-group OutsidetoDMZ in interface Outside`**Примечание:** Помните, можно только применить один список доступа для интерфейса для направления. Если вам уже применились к входящему ACL внешний интерфейс, вы не можете применить ACL данного примера к нему. Вместо этого добавьте записи ACE, в этом примере в текущий список контроля доступа, активированный на интерфейсе.**Примечание:** Чтобы отключить FTP-трафик, например, из Интернета в DMZ, используйте следующую команду:`ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`**Совет:** При изменении конфигурации NAT рекомендуется удалить текущие преобразования NAT. **Таблицу преобразования NAT можно очистить с помощью команды clear xlate. Но будьте осторожны при выполнении этой операции, поскольку очистка таблицы преобразования приведет к разрыву всех текущих подключений, использующих записи преобразования.** Можно избежать очистки таблицы преобразования, подождав истечения времени ожидания текущих записей преобразования, но это не рекомендуется, поскольку непредвиденные операции могут привести к созданию новых соединений на основе новых правил.

Внутренняя сеть/DMZ — Интернет

В этом сценарии хостам, расположенным на внутреннем интерфейсе (Безопасность 100) устройства безопасности, предоставляют доступ к Интернету на внешнем интерфейсе (Безопасность 0). Это достигается с помощью преобразования PAT (перегрузки NAT), формы динамического преобразования NAT. В отличие от других сценариев список контроля доступа не требуется в этом случае, так как хосты, подключенные к интерфейсу с более высоким уровнем безопасности, могут получать доступ к хостам, подключенным к менее безопасному интерфейсу.

1. Укажите источники трафика для преобразования. **Здесь задано правило NAT № 1 и**

весь трафик от хостов во внутренней сети и DMZ разрешен.
```
ASA-AIP-CLI(config)# nat (inside) 1 172.20.1.0255.255.255.0ASA-AIP-CLI(config)# nat (inside) 1 192.168.1.0255.255.255.0
```

2. Укажите, какой адрес, пул адресов или интерфейс будет использоваться преобразованным трафиком NAT для обращения к интерфейсу. В этом случае выполняется преобразование PAT на одном из внешний интерфейсов. Это будет особенно полезно, когда адрес внешнего интерфейса неизвестен заранее, например, в конфигурации DHCP. **Здесь глобальная команда вводится с тем же идентификатором NAT 1 и привязывает его к правилам NAT того же идентификатора.**
```
ASA-AIP-CLI(config)# global (Outside) 1interface
```

Совет: При изменении конфигурации NAT рекомендуется удалить текущие преобразования NAT. **Таблицу преобразования NAT можно очистить с помощью команды clear xlate. Но будьте осторожны при выполнении этой операции, поскольку очистка таблицы преобразования приведет к разрыву всех текущих подключений, использующих записи преобразования.** Можно избежать очистки таблицы преобразования, подождав истечения времени ожидания текущих записей преобразования, но это не рекомендуется, поскольку непредвиденные операции могут привести к созданию новых соединений на основе новых правил.

Примечание: Чтобы заблокировать трафик из более безопасной зоны (внутренней сети) в менее безопасную зону (Интернет или DMZ), создайте список контроля доступа и примените его к внутреннему интерфейсу PIX/ASA как входящий.

Примечание: Пример: Для блокирования трафика порта 80 от хоста 172.20.1.100 на внутренней сети к Интернету используйте это:

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

Та же связь уровня безопасности

Начальная конфигурация показывает, что интерфейсы "DMZ" и "DMZ-2-testing" настроены с уровнем безопасности (50); по умолчанию эти два интерфейса не могут говорить. Здесь мы позволяем этим интерфейсам говорить с этой командой:

```
ASA-AIP-CLI(config)# same-security-traffic permit inter-interface
```

Примечание: Даже если команда "same-security traffic permit inter-interface" задана на интерфейсах с одинаковым уровнем безопасности ("DMZ" и"DMZ-2-testing"), необходимо задать правило преобразования (статического или динамического), чтобы разрешить доступ к ресурсам, подключенным к этим интерфейсам.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Поиск и устранение неполадок соединений через PIX и ASA
- Конфигурации NATПроверка и устранение неполадок NAT

Дополнительные сведения

- Справочник по командам Cisco ASA
- Справочник по командам Cisco PIX
- Системные сообщения и сообщения об ошибках Cisco ASA
- Системные сообщения и сообщения об ошибках Cisco PIX
- Cisco Systems – техническая поддержка и документация