ASA 7.x/PIX 6.x и более поздние: Пример настройки открытия и блокировки портов

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Родственные продукты
Условные обозначения
Настройка
Схема сети
Блокирование портов конфигурация
Открытие портов конфигурация
Конфигурация через ASDM
Проверка
Устранение неполадок
Дополнительные сведения

Введение

В этом документе приводится пример конфигурации для открытия или блокировки портов для различных видов трафика, таких как http или ftp, в устройстве защиты.

Примечание: Сроки "открытие порта" и "разрешение порта" отправляют то же значение. Точно так же "блокирование порта" и "ограничение порта" также отправляют то же значение.

Предварительные условия

Требования

Этот документ предполагает, что PIX/ASA настроен и работает должным образом.

Используемые компоненты

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

- Устройство адаптивной защиты (ASA) серии 5500 Cisco, которое выполняет версию 8.2 (1)

- Cisco Adaptive Security Device Manager (ASDM) версия 6.3 (5)

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 с Cisco Устройство Межсетевого экрана PIX серии 500 с версией программного обеспечения 6.x и выше.

Условные обозначения

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

Настройка

Каждый интерфейс должен иметь уровень безопасности от 0 (самый низкий) к 100 (самый высокий). Например, необходимо назначить большую часть защищенной сети, такой как сеть внутреннего хоста, к уровню 100. В то время как внешняя сеть, которая связана с Интернетом, может быть уровнем 0, другие сети, такие как DMZs, могут быть расположены промежуточные. Можно назначить несколько интерфейсов на тот же уровень безопасности.

По умолчанию все порты заблокированы на внешнем интерфейсе (уровень безопасности 0), и все порты открыты на внутреннем интерфейсе (уровень безопасности 100) устройства безопасности. Таким образом весь исходящий трафик может пройти через устройство безопасности без любой конфигурации, но входящий трафик может быть позволен конфигурацией списка доступа и статических команд в устройстве безопасности.

Примечание: В целом все порты заблокированы от Более низкой Зоны безопасности до Зоны Более высокой безопасности, и все порты открыты от Зоны Более высокой безопасности до Более низкой Зоны безопасности, если это проверка трафика потоком включено для обоих входящих и исходящих трафиков.

Этот раздел состоит из подразделов как показано:

- Схема сети
- Блокирование портов конфигурация
- Открытие портов конфигурация

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 настоящем документе используется следующая схема сети:

Блокирование портов конфигурация

Устройство безопасности позволяет любой исходящий трафик, пока это явно не заблокировано расширенным списком доступа.

Список доступа составлен из одной или более Записей управления доступом. Зависящий от типа списка доступа, можно задать адреса источника и назначения, протокол, порты (для TCP или UDP), тип ICMP (для ICMP), или EtherType.

Примечание: Для протоколов без установления соединения, таких как ICMP, устройство безопасности устанавливает однонаправленные сеансы, таким образом, вы любая потребность списки доступа для разрешения ICMP в обоих направлениях (приложением списков доступа к источнику и интерфейсам назначения), или необходимо включить механизм Инспектирования icmp. Механизм Инспектирования icmp рассматривает сеансы ICMP как двунаправленные подключения.

Выполните эти шаги для блокирования портов, которые обычно применяются к трафику, который происходит из внутренней части (зона более высокой безопасности) к DMZ (более низкая зона безопасности) или DMZ к внешней стороне.

1. Создайте Список контроля доступа таким способом, которым вы блокируете трафик указанного порта.
   access-list <name> extended deny <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number> access-list <name> extended permit ip any any
2. Затем свяжите access-list с **командой access-group**, чтобы быть активными.
   access-group <access list name> in interface <interface name>

Примеры:

1. **Заблокируйте трафик порта HTTP:** для блокирования внутренней сети 10.1.1.0 от доступа до http (Web-сервер) с IP 172.16.1.1 размещенных в сети DMZ, создайте ACL как показано:`ciscoasa(config)#`**`access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80`** `ciscoasa(config)#`**`access-list 100 extended permit ip any any`** `ciscoasa(config)#`**`access-group 100 in interface inside`** **Примечание:** Используйте **не** придерживавшийся командами списка доступа для удаления блокирования порта.
2. **Заблокируйте трафик порта FTP:** для блокирования внутренней сети 10.1.1.0 от доступа до FTP (файловый сервер) с IP 172.16.1.2 размещенных в сети DMZ, создайте ACL как показано:`ciscoasa(config)#`**`access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21`** `ciscoasa(config)#`**`access-list 100 extended permit ip any any`** `ciscoasa(config)#`**`access-group 100 in interface inside`**

Примечание: См. порты IANA для узнавания больше информации о назначениях порта.

Пошаговую конфигурацию для выполнения этого через ASDM показывают в этом разделе.

1. Перейдите **к Конфигурации> Межсетевой экран> Правила Доступа**. **Нажмите Add Правило Доступа** создать access-list.
2. Определите источник и назначение и действие правила доступа наряду с интерфейсом, что будет привязано это правило доступа. Выберите подробные данные для выбора определенного порта для блокирования.
3. Выберите **http** из списка доступных портов, затем нажмите **OK** для возвращения назад к окну Add Access Rule.

4. Нажмите **OK** для завершения конфигурации правила доступа.
5. Нажмите **Insert After** для добавления правила доступа к тому же access-list.
6. Разрешите, чтобы трафик от "любого" до "любого" для предотвращения "Неявный запретил". Затем нажмите **OK** для завершения добавления этого правила доступа.
7. Настроенный access-list может быть замечен во вкладке Access Rules. Нажмите **Apply** для передачи этой конфигурации к Устройству безопасности.Конфигурация, передаваемая от ASDM, приводит к этому набору команд на Интерфейсе командной строки (CLI) ASA.`access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www`
`access-list inside_access_in extended permit ip any any`
`access-group inside_access_in in interface inside`Посредством этих шагов пример 1 был выполнен через ASDM для блокирования 10.1.1.0 сетей от доступа к Web-серверу, 172.16.1.1. Пример 2 может также быть достигнут таким же образом для блокирования всех 10.1.1.0 сетей от доступа к серверу FTP, 172.16.1.2. Единственная разница будет при выборе порта.**Примечание:** Эта конфигурация правила доступа, например, 2, как предполагается, является новой конфигурацией.
8. Определите правило доступа для блокирования трафика FTP, затем нажмите вкладку **Details** для выбора порта назначения.
9. Выберите порт **ftp** и нажмите **OK** для возвращения назад к окну Add Access Rule.
10. Нажмите **OK** для завершения конфигурации правила доступа.
11. Добавьте другое правило доступа разрешить любой другой трафик. В противном случае Неявные Запрещают правило, заблокирует весь трафик на этом интерфейсе.
12. Настройка списка полного доступа похожа на это под вкладкой Access Rules.
13. Нажмите **Apply** для передачи конфигурации к ASA. Эквивалентная конфигурация CLI похожа на это:`access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp`
`access-list inside_access_in extended permit ip any any`
`access-group inside_access_in in interface inside`

Открытие портов конфигурация

Устройство безопасности не позволяет входящего трафика, пока это явно не разрешено расширенным списком доступа.

Если вы хотите позволить внешнему хосту обращаться к внутреннему хосту, можно применить список доступа на вход на внешний интерфейс. Необходимо задать транслированный адрес внутреннего хоста в списке доступа, потому что транслированный адрес является адресом, который может использоваться на внешней сети. Выполните эти шаги для открытия портов от более низкой зоны безопасности до зоны более высокой безопасности. Например, позвольте трафик с внешней стороны (более низкая зона безопасности) к внутреннему интерфейсу (зона более высокой безопасности) или DMZ к внутреннему интерфейсу.

1. Статическая запись NAT создает фиксированное преобразование фактического адреса в назначенный адрес. Этот сопоставленный адрес является адресом, который размещает в Интернете и может использоваться для доступа к серверу приложений на DMZ без потребности знать действительный адрес сервера.
`static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] | access-list access_list_name | interface}` См. Статический NAT раздел Справочника по командам для PIX/ASA для узнавания больше информации.

2. Создайте ACL для разрешения определенного трафика порта.
   access-list <name> extended permit <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number>
3. Свяжите access-list с **командой access-group**, чтобы быть активными.
   access-group <access-list name> in interface <interface name>

Примеры:

1. **Откройте трафик порта SMTP:** Откройте **порт tcp 25**, чтобы позволить хостам от внешнего (Интернет) обращаться к почтовому серверу, размещенному в сеть DMZ.Команда **Static** сопоставляет внешний адрес 192.168.5.3 с реальным адресом DMZ 172.16.1.3.`ciscoasa(config)#`**`static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255`** `ciscoasa(config)#`**`access-list 100 extended permit tcp any host 192.168.5.3 eq 25`** `ciscoasa(config)#`**`access-group 100 in interface outside`**
2. **Откройте трафик порта HTTPS:** Откройте **порт tcp 443**, чтобы позволить хостам от внешнего (Интернет) обращаться к Web-серверу (безопасному) размещенный в сеть DMZ.`ciscoasa(config)#`**`static (DMZ,Outside) 192.168.5.5 172.16.1.5 netmask 255.255.255.255`**
   `ciscoasa(config)#`**`access-list 100 extended permit tcp any host 192.168.5.5 eq 443`**
   `ciscoasa(config)#`**`access-group 100 in interface outside`**
3. **Позвольте трафик DNS:** Откройте **порт udp 53**, чтобы позволить хостам от внешнего (Интернет) обращаться к серверу DNS (безопасному) размещенный в сеть DMZ.`ciscoasa(config)#`**`static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255`**
   `ciscoasa(config)#`**`access-list 100 extended permit udp any host 192.168.5.4 eq 53`**
   `ciscoasa(config)#`**`access-group 100 in interface outside`**

Примечание: См. порты IANA для узнавания больше информации о назначениях порта.

Конфигурация через ASDM

Пошаговый подход для выполнения вышеупомянутых задач через ASDM показывают в этом разделе.

1. Создайте правило доступа разрешить трафик SMTP к 192.168.5.3 серверам.
2. Определите источник и назначение правила доступа и интерфейс, с которым связывает это правило. Кроме того, определите Действие как **Разрешение**.
3. Выберите **SMTP** в качестве порта, затем нажмите **OK**.
4. Нажмите **OK** для завершения настройки правила доступа.
5. Настройте статическое NAT для перевода 172.16.1.3 в 192.168.5.3Перейдите **к Конфигурации> Межсетевой экран>, Правила NAT> Добавляют Статическое NAT Правило** для добавления статической записи NAT.Выберите Original Source и Преобразованный IP-адрес наряду с их связанными интерфейсами, затем нажмите **OK**, чтобы закончить настраивать Статическое NAT правило.Этот образ изображает все три статических правила, которые перечислены в разделе В качестве примера:Этот образ изображает все три правила доступа, которые перечислены в разделе В качестве примера:

Проверка

Можно проверить с **некоторыми командами show**, как показано:

- **show xlate** информация о текущем преобразовании показа
- **show access-list** — счетчики попаданий показа для политики доступа

- **show logging** журналы в буфере.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Устранение неполадок

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

Дополнительные сведения

- PIX/ASA 7.X : Включение/отключение связи между интерфейсами
- PIX 7.0 и перенаправление (пересылка) портов адаптированного устройства безопасности с помощью команд nat, global, static, conduit и access-list
- "Использование команд nat, global, static, conduit и access-list и переназначене порта (перенаправление) на PIX"
- PIX/ASA 7.x: пример включения служб FTP/TFTP
- PIX/ASA 7.x: Пример настройки служб для включения VoIP (SIP, MGCP, H323, SCCP)
- PIX/ASA 7.x: Mail Server Access on the DMZ Configuration Example
- Cisco Systems – техническая поддержка и документация