Настройте ASA для избыточных или резервных каналов поставщика

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Родственные продукты](#)
[Общие сведения](#)
[Обзор характеристики отслеживания статического маршрута](#)
[Важные рекомендации](#)
[Настройка](#)
[Схема сети](#)
[Конфигурация интерфейса командой строки CLI](#)
[Настройка посредством ASDM](#)
[Проверка](#)
[Подтвердите, что Конфигурация Завершена](#)
[Подтвердите, что Резервный маршрут Установлен (Метод CLI)](#)
[Подтвердите, что Резервный маршрут Установлен (Метод ASDM)](#)
[Устранение неполадок](#)
[Команды "debug"](#)
[Ненужное удаление отслеживаемого маршрута](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить многофункциональное устройство защиты Cisco ASA серии 5500 (ASA) для использования характеристики отслеживания статического маршрута, чтобы позволить устройству использовать избыточные или резервные Интернет-соединения.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- 5555-X Серия Cisco ASA, которая работает под управлением ПО версии 9.x или позже
- Версия Cisco ASDM 7.x или позже

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

Можно также использовать эту конфигурацию с Версией 9.1 (5) серии 5500 Cisco ASA.

> **Примечание: Команда резервного интерфейса** требуется для настройки четвертого интерфейса на серии ASA 5505. См. раздел резервного интерфейса *Справочника по командам Cisco Security Appliance, Версия 7.2* для получения дополнительной информации.

Общие сведения

Этот раздел предоставляет обзор характеристики отслеживания статического маршрута, которая описана в этом документе, а также некоторых важных рекомендациях перед началом.

Обзор характеристики отслеживания статического маршрута

Одна проблема с использованием статических маршрутов состоит в том, что никакой свойственный механизм не существует, который может определить, подключен ли маршрут или вниз. Маршрут остается в таблице маршрутизации, даже если шлюз следующего перехода становится недоступен. Статические маршруты удаляются из таблицы маршрутизации, только если соответствующий интерфейс в устройстве безопасности прекращает работу. Для решения этой проблемы характеристика отслеживания статического маршрута используется для отслеживания доступности статического маршрута. Функция удаляет статический маршрут из таблицы маршрутизации и заменяет его резервным маршрутом после сбоя.

Отслеживание статического маршрута позволяет ASA использовать недорогое соединение со вторичным интернет-провайдером, если основная выделенная линия становится недоступной. Для достижения этого резервирования ASA привязывает статический маршрут к контролирующей цели, которую вы определяете. Операция Соглашения об уровне обслуживания (SLA) контролирует цель с периодическими эхо-запросами протокола ICMP. Если эхо - ответ не получено, то объект рассматривают вниз, и связанный маршрут удален из таблицы маршрутизации. А вместо удаленного маршрута используется ранее

настроенный резервный маршрут. В то время как резервный маршрут используется, операция монитора SLA продолжает свои попытки достигнуть контролирующей цели. Когда целевой объект снова становится доступен, первый маршрут возвращается в таблицу маршрутизации, а резервный маршрут удаляется.

В примере, который используется в этом документе, ASA поддерживает два соединения с Интернетом. Первое подключение — это высокоскоростная выделенная линия, доступная через маршрутизатор, предоставленный основным поставщиком. Вторым соединением является Цифровая абонентская линия (DSL) меньшей скорости, к которой обращаются через модем DSL, предоставленный вторичным интернет-провайдером.

> **Примечание:** Конфигурация, которая описана в этом документе, не может использоваться для распределения нагрузки или распределения нагрузки, поскольку это не поддерживается на ASA. Используйте эту конфигурацию только для обеспечения избыточности или резервирования. Если основной отказывает, исходящий трафик использует основного поставщика услуг Интернет, и затем вторичного интернет-провайдера. Сбой основного поставщика приводит в временному прекращению потока трафика.

DSL-подключение не используется, пока активна выделенная линия и доступен шлюз основного поставщика. Однако, если соединение с основным поставщиком услуг Интернет выключается, ASA изменяет таблицу маршрутизации для направления трафик к подключению DSL. Отслеживание статического маршрута используется для достижения этого резервирования.

ASA настроен со статическим маршрутом, который направляет весь интернет-трафик к основному поставщику услуг Интернет. Каждые десять секунд процесс монитора SLA проверяет, чтобы подтвердить, что шлюз основного поставщика достижим. Если выясняется, что шлюз основного поставщика недоступен, статический маршрут, по которому трафик направляется в этот интерфейс, удаляется из таблицы маршрутизации. Чтобы заменить этот статический маршрут, устанавливается другой статический маршрут, направляющий трафик вспомогательному поставщику. Этот альтернативный статический маршрут направляет трафик вспомогательному поставщику по DSL-модему до тех пор, пока канал основного поставщика не станет доступен.

Эта конфигурация предоставляет относительно недорогой способ гарантировать, что исходящий доступ в Интернет остается доступным пользователям позади ASA. Как описано в этом документе, эта настройка не могла бы подойти для входящего доступа для ресурсов позади ASA. Усовершенствованные сетевые навыки требуются для достижения бесшовных входящих подключений. Эти навыки не рассматриваются в этом документе.

Важные рекомендации

Перед попыткой конфигурации, которая описана в этом документе, необходимо выбрать контролирующую цель, которая может ответить на запросы эха Протокола ICMP. Цель может быть любым сетевым объектом, который вы выбираете, но рекомендуется цель, которая близко связана к вашему соединению интернет-провайдера (ISP). Вот некоторые возможные цели мониторинга:

- Адрес шлюза поставщика

- Другой управляемый ИНТЕРНЕТ-ПРОВАЙДЕРОМ адрес
- Сервер в другой сети, такой как аутентификация, авторизация и учет (AAA), с которой должен связаться ASA
- Персистентный сетевой объект в другой сети (рабочий стол или портативный компьютер, которого можно завершить работу ночью, не являются хорошим выбором),

Этот документ предполагает, что ASA полностью в рабочем состоянии и настроен, чтобы позволить Cisco Adaptive Security Device Manager (ASDM) изменять конфигурацию.

> **Совет:** Для получения информации о том, как позволить ASDM настраивать устройство, ссылаться на Доступ HTTPS Настройки для раздела ASDM *Книги 1 CLI: Руководство Конфигурации интерфейса командой строки Общих функционирований Серии Cisco ASA, 9.1*.

Настройка

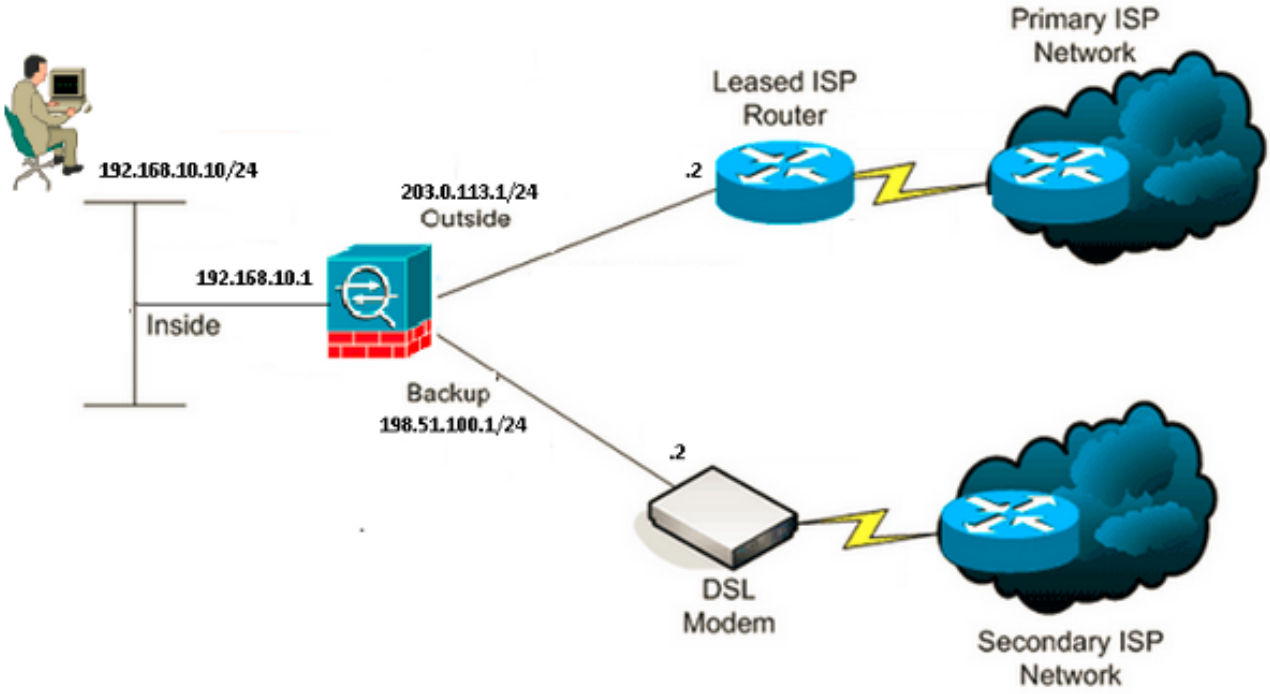
Используйте информацию, которая описана в этом разделе для настройки ASA для использования характеристики отслеживания статического маршрута.

> **Примечание:** Используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты) для получения дополнительных сведений о командах, которые используются в этом разделе.

> **Примечание:** IP-адреса, которые используются в этой конфигурации, не юридически маршрутизируемы в Интернете. Это адреса RFC 1918 , которые используются в лабораторной среде.

Схема сети

Пример, который предоставлен в этом разделе, использует эту сетевую установку:



Конфигурация интерфейса командой строки CLI

Используйте эту информацию для настройки ASA через CLI:

```
ASA#show running-config

ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0

!--- The interface attached to the Secondary ISP.
!--- "backup" was chosen here, but any name can be assigned.

!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
```

```
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone IND 5 30
object network Inside_Network
 subnet 192.168.10.0 255.255.255.0
object network inside_network
 subnet 192.168.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface

!--- NAT Configuration for Outside and Backup

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1

!--- Enter this command in order to track a static route.
!--- This is the static route to be installed in the routing
!--- table while the tracked object is reachable. The value after
!--- the keyword "track" is a tracking ID you specify.

route backup 0.0.0.0 0.0.0.0 198.51.100.2 254

!--- Define the backup route to use when the tracked object is unavailable.
!--- The administrative distance of the backup route must be greater than
!--- the administrative distance of the tracked route.
!--- If the primary gateway is unreachable, that route is removed
!--- and the backup route is installed in the routing table
!--- instead of the tracked route.

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
```

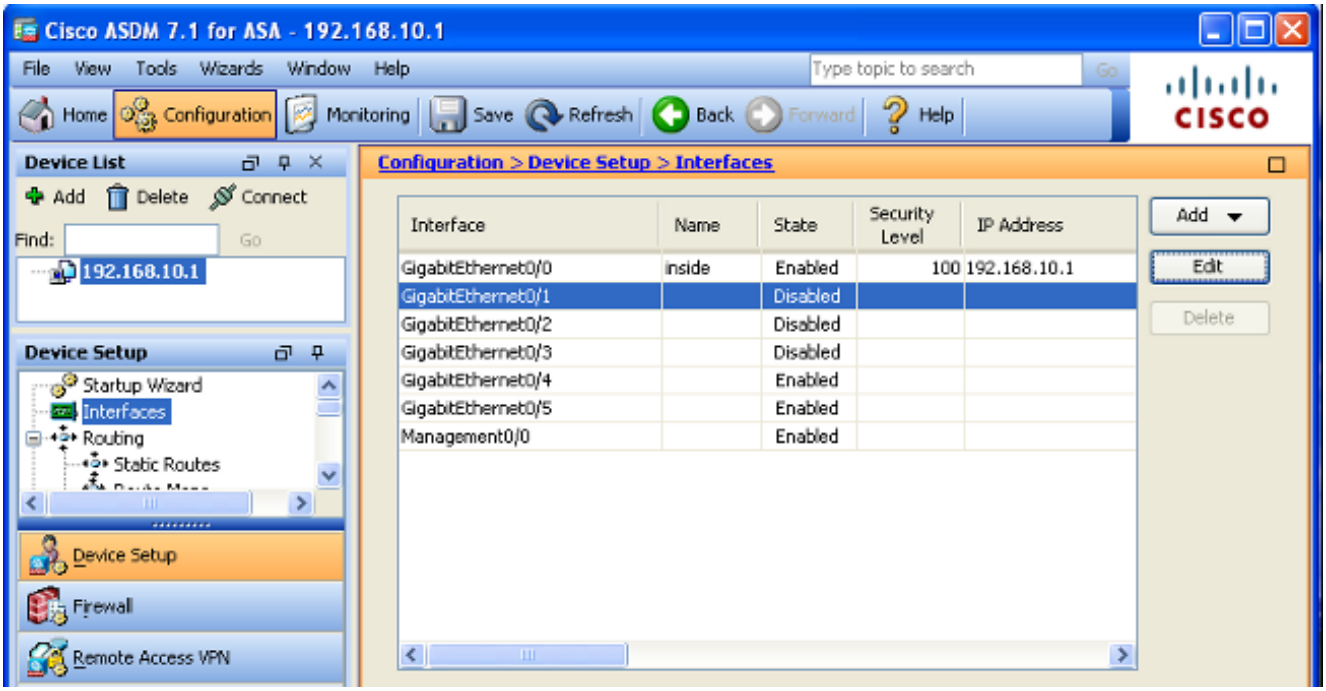
```
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10

!--- Configure a new monitoring process with the ID 123. Specify the
!--- monitoring protocol and the target network object whose availability the tracking
!--- process monitors. Specify the number of packets to be sent with each poll.
!--- Specify the rate at which the monitor process repeats (in seconds).

sla monitor schedule 123 life forever start-time now

!--- Schedule the monitoring process. In this case the lifetime
!--- of the process is specified to be forever. The process is scheduled to begin
!--- at the time this command is entered. As configured, this command allows the
!--- monitoring configuration specified above to determine how often the testing
!--- occurs. However, you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times.

crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability

!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry. 123 is the ID of the SLA process
!--- defined above.

telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 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 rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
```

```
 inspect icmp
!
service-policy global_policy global
```

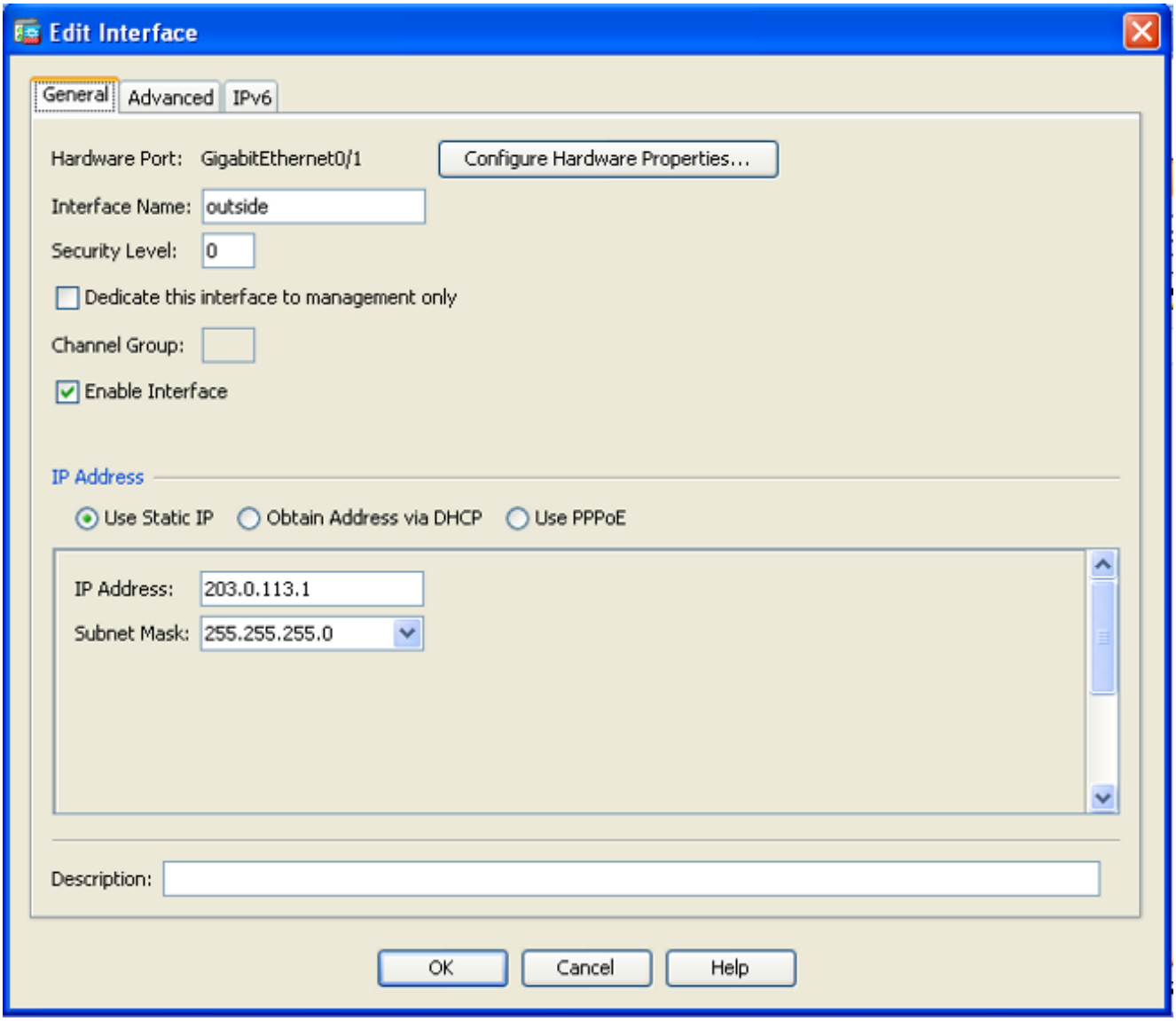
Настройка посредством ASDM

Выполните эти шаги для настройки избыточной или резервной поддержки интернет-провайдера с приложением ASDM:

1. В рамках приложения ASDM нажмите **Configuration**, и затем нажмите **Interfaces**.



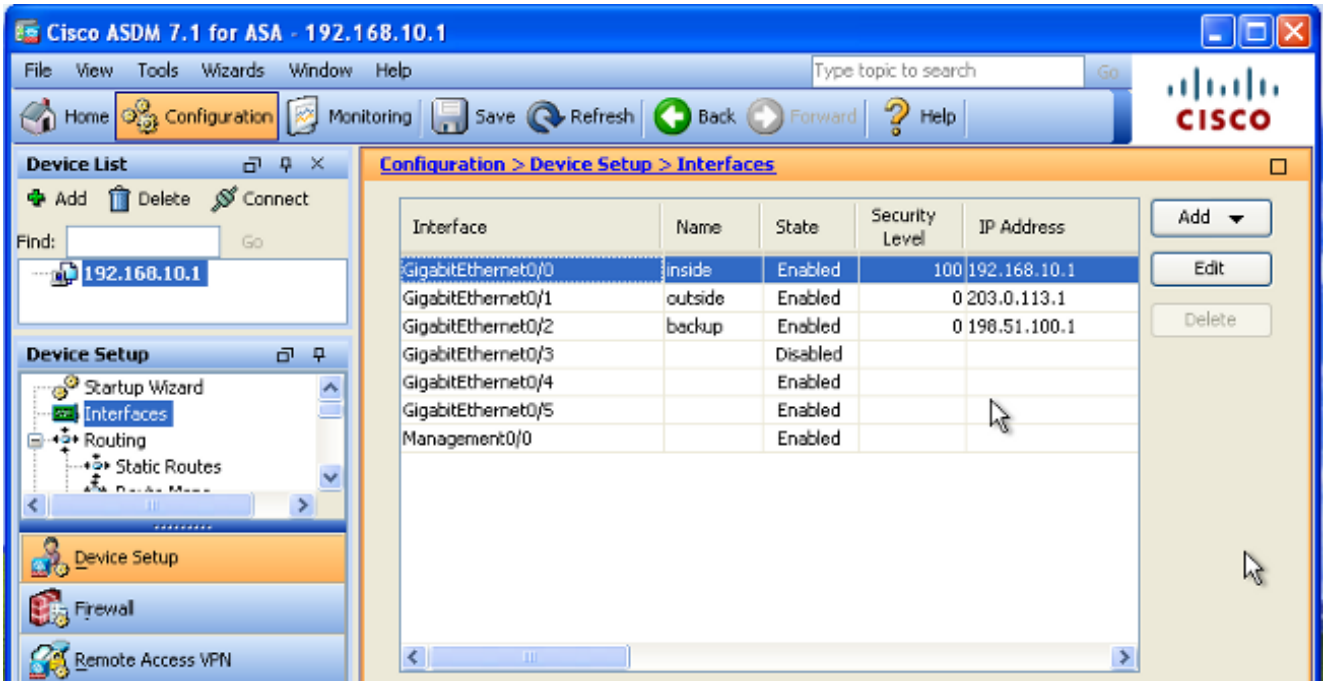
2. Выберите **GigabitEthernet0/1** из списка Интерфейсов, и затем нажмите **Edit** . Появится следующее диалоговое окно:



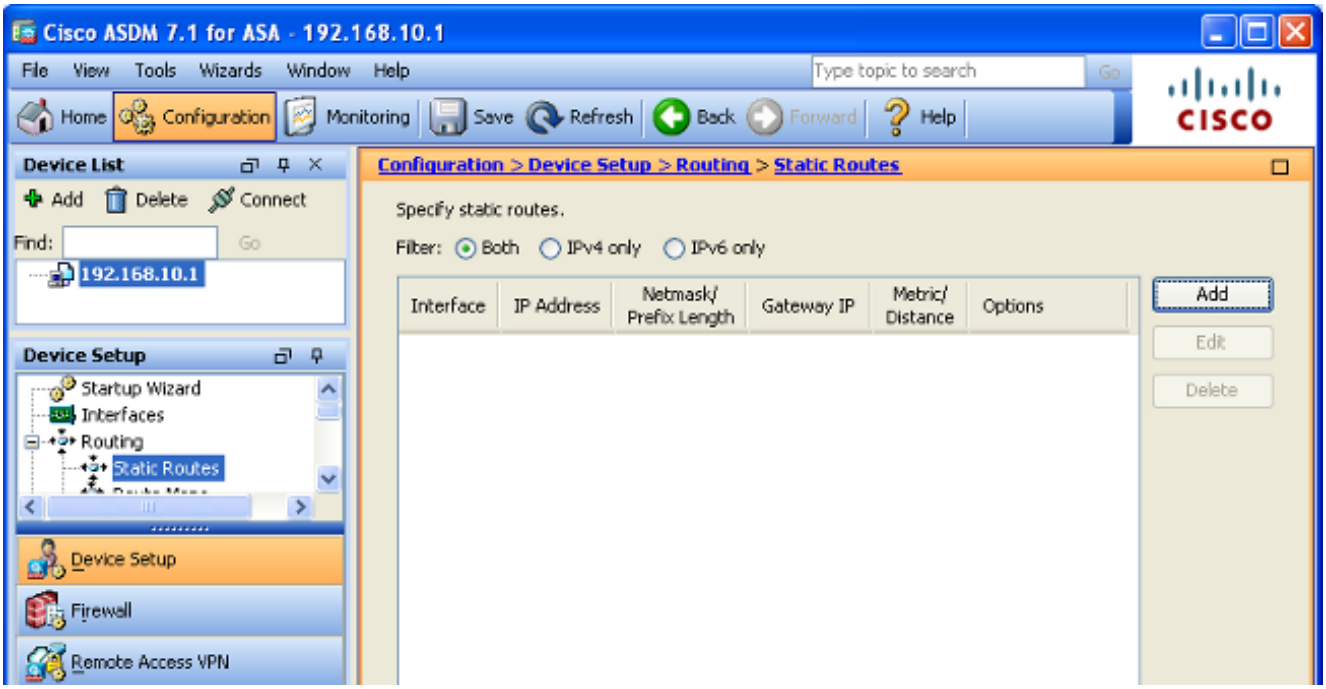
3. Установите **Разрешать** флажок **Проверки интерфейса** и введите соответствующие значения в *Имя интерфейса*, *Уровень безопасности*, *IP-адрес* и поля *Subnet Mask*.

4. **Нажмите кнопку ОК, чтобы закрыть диалоговое окно.**

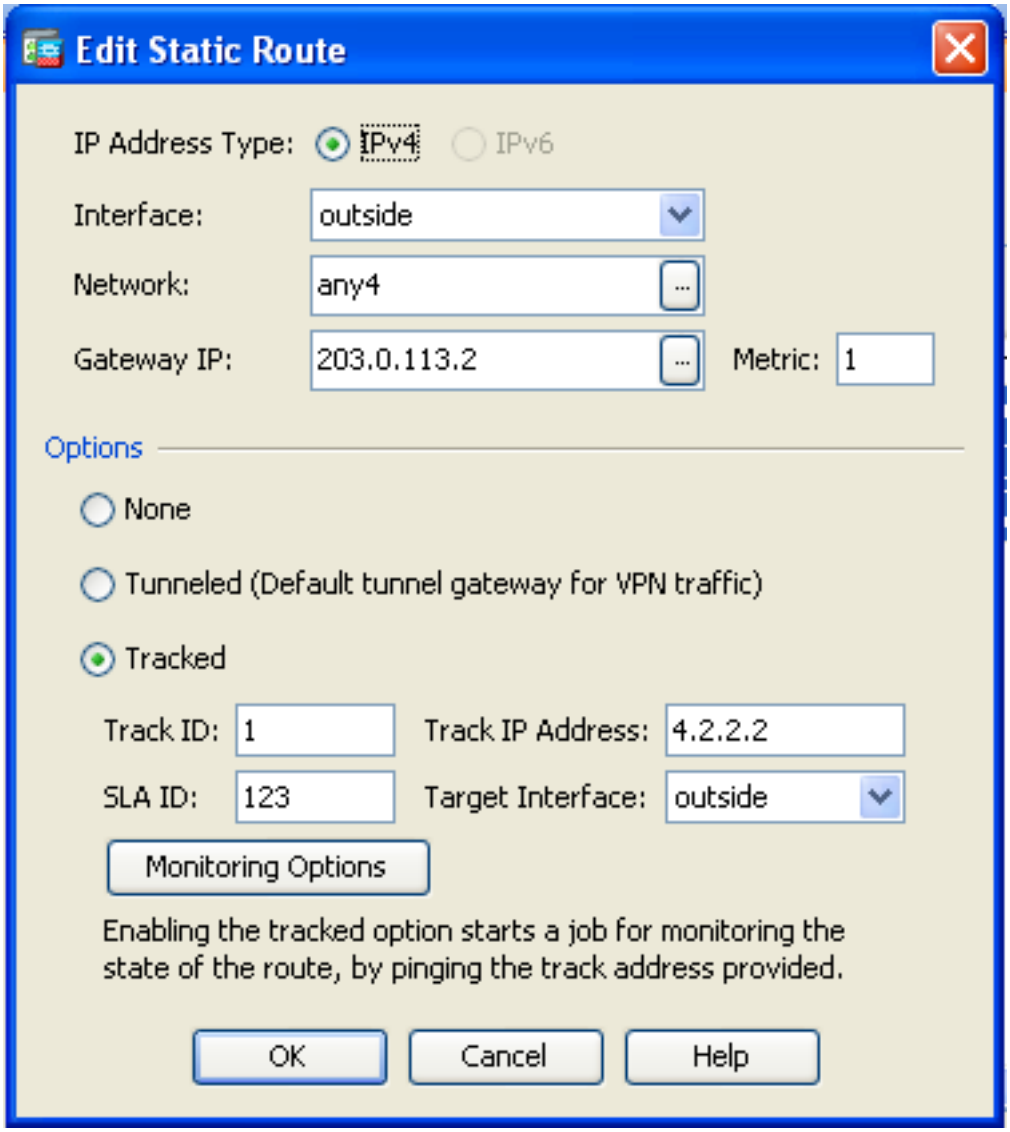
5. Настройте другие интерфейсы по мере необходимости, и затем нажмите **Apply** для обновления конфигурации ASA:



6. Выберите **Routing** и нажмите **Static Routes**, расположенный на левой части приложения ASDM:



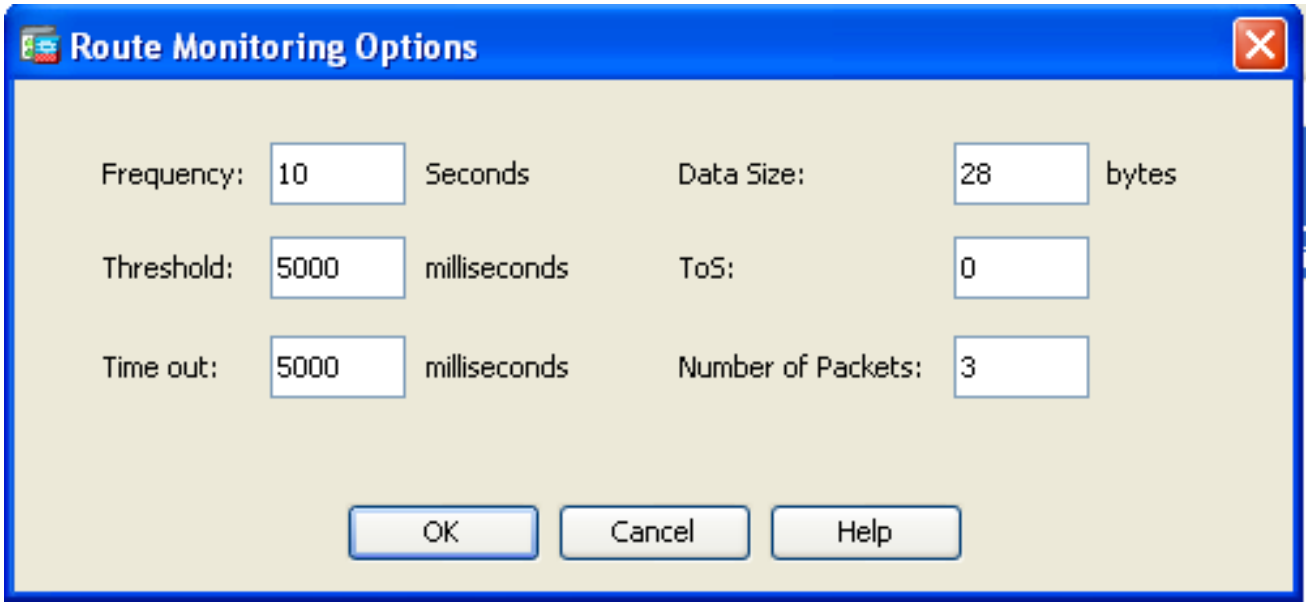
7. **Нажмите кнопку Add, чтобы добавить новые статические маршруты.** Появится следующее диалоговое окно:



8. Из раскрывающегося списка "Interface Name" выберите интерфейс для маршрута и настройте стандартный маршрут для достижения шлюза. В данном примере, **203.0.113.2** шлюз основного поставщика, и **4.2.2.2** объект для мониторинга с эхо - запрос ICMP.

9. В области Options нажмите кнопку с зависимой фиксацией **Tracked** и введите соответствующие значения в *ID Дорожки*, *ID SLA* и *поля IP Address Дорожки*.

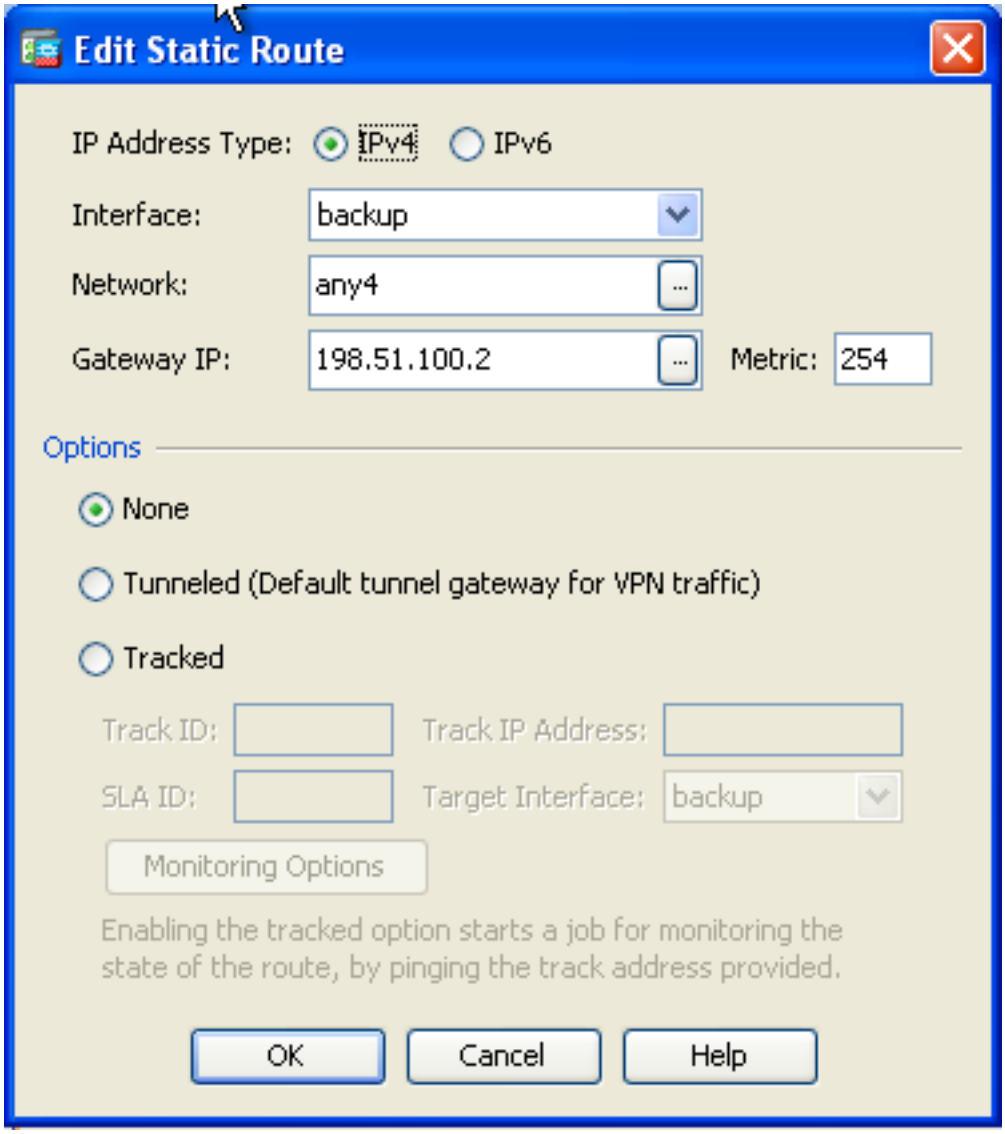
10. **Нажмите кнопку Monitoring Options.** Появится следующее диалоговое окно:



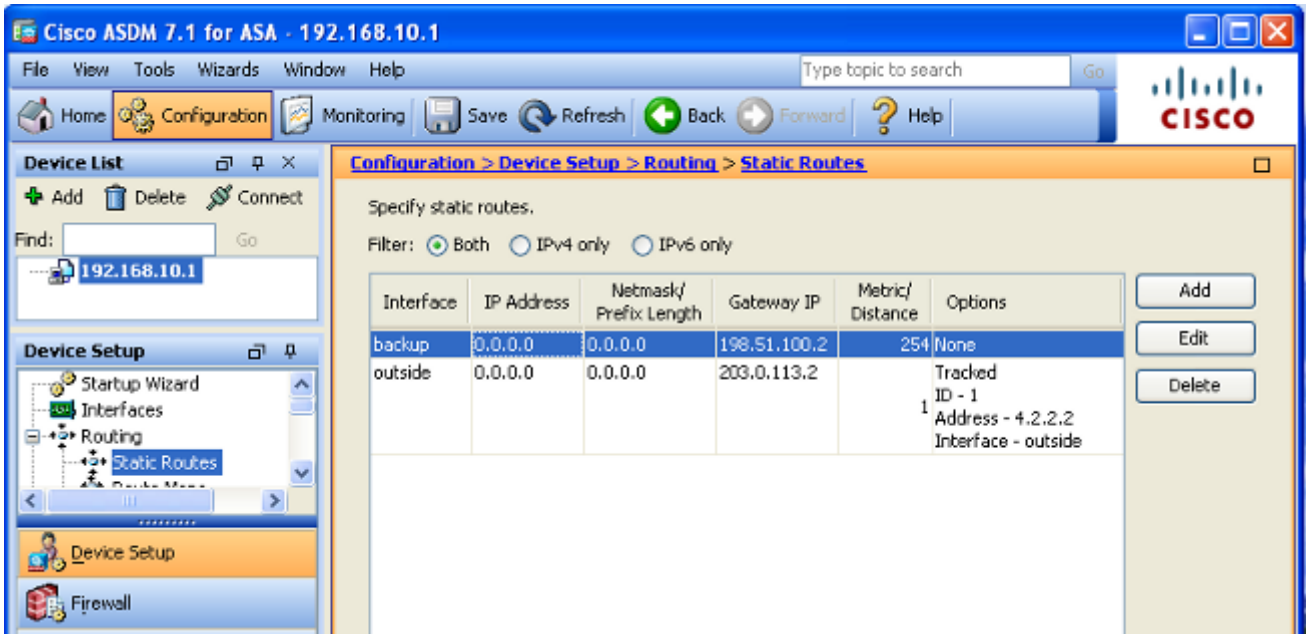
11. Введите соответствующие значения для частоты и других опций мониторинга, и затем нажмите **OK**.

12. Добавьте другой статический маршрут для вспомогательного поставщика, чтобы обеспечить маршрут для выхода в Интернет. Чтобы сделать этот маршрут вспомогательным, установите для него более высокую метрику, например 254. В случае сбоя основного маршрута (основного поставщика) неработающий маршрут будет удален из таблицы маршрутизации. Этот дополнительный маршрут (вторичный интернет-провайдер) установлен в таблице маршрутизации Обмена через закрытый Интернет (PIX) вместо этого.

13. **Нажмите кнопку OK, чтобы закрыть диалоговое окно:**



Конфигурации появятся в списке интерфейсов:



14. Выберите настройку маршрутизации, и затем нажмите **Apply** для обновления конфигурации ASA.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Подтвердите, что Конфигурация Завершена

> **Примечание:** Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Используйте эти **команды показа**, чтобы проверить, что ваша конфигурация завершена:

- **монитор SLA show running config** – выходные данные этой команды отображают команды SLA в конфигурации.
```
ASA# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```
- **покажите конфигурацию монитора SLA** – выходные данные этой команды отображают параметры настройки текущей конфигурации операции.
```
ASA# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 4.2.2.2
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data&colon; No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```
- **покажите операционное состояние монитора SLA** – выходные данные этой команды отображают в рабочем состоянии статистику операции SLA.

  До сбоя основного поставщика рабочее состояние выглядит так:
```
ASA# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:30:40.672 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 46
```

```
    Number of operations skipped: 0
    Current seconds left in Life: Forever
    Operational state of entry: Active
    Last time this entry was reset: Never
    Connection loss occurred: FALSE
    Timeout occurred: FALSE
    Over thresholds occurred: FALSE
    Latest RTT (milliseconds): 1
    Latest operation start time: 13:38:10.672 IND Sun Jan 4 2015
    Latest operation return code: OK
    RTT Values:
    RTTAvg: 1      RTTMin: 1      RTTMax: 1
    NumOfRTT: 3    RTTSum: 3      RTTSum2: 3
```

После сбоев основного поставщика услуг Интернет (и таймаут эхо - запрос ICMP), это - операционное состояние:

```
ASA# show sla monitor operational-state
Entry number: 123
Modification time: 13:30:40.671 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 57
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 13:40:00.672 IND Sun Jan 4 2015
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0      RTTMin: 0      RTTMax: 0
NumOfRTT: 0    RTTSum: 0      RTTSum2: 0
```

Подтвердите, что Резервный маршрут Установлен (Метод CLI)

Введите **команду show route**, чтобы подтвердить, что установлен резервный маршрут.

Перед сбоями основного поставщика услуг Интернет таблица маршрутизации кажется подобной этому:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 203.0.113.2 to network 0.0.0.0

C   203.0.113.0 255.255.255.0 is directly connected, outside
C   192.168.10.0 255.255.255.0 is directly connected, inside
C   198.51.100.0 255.255.255.0 is directly connected, backup
S*  0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

После сбоев основного поставщика услуг Интернет удален статический маршрут, и резервный маршрут установлен, таблица маршрутизации кажется подобной этому:

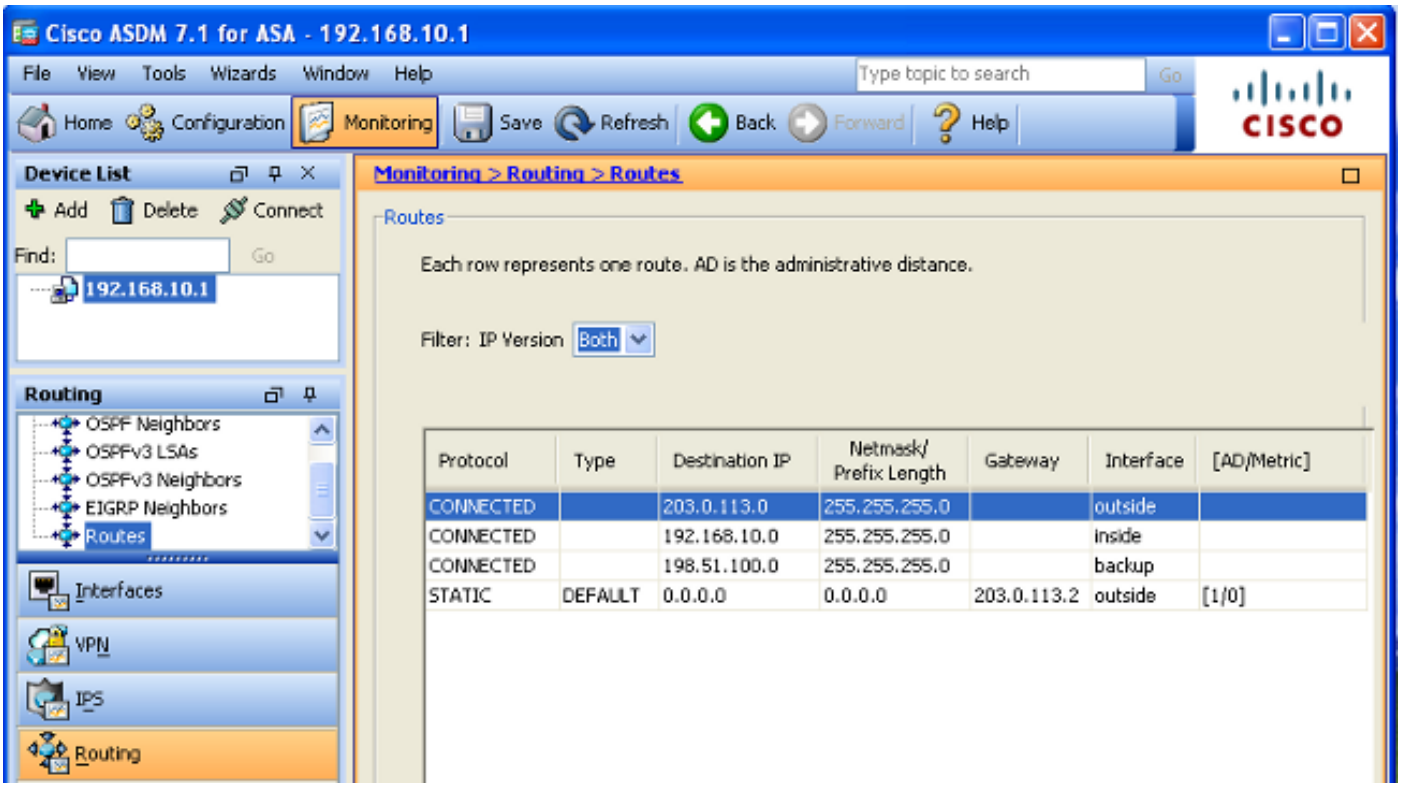
```
ASA# show route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 198.51.100.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

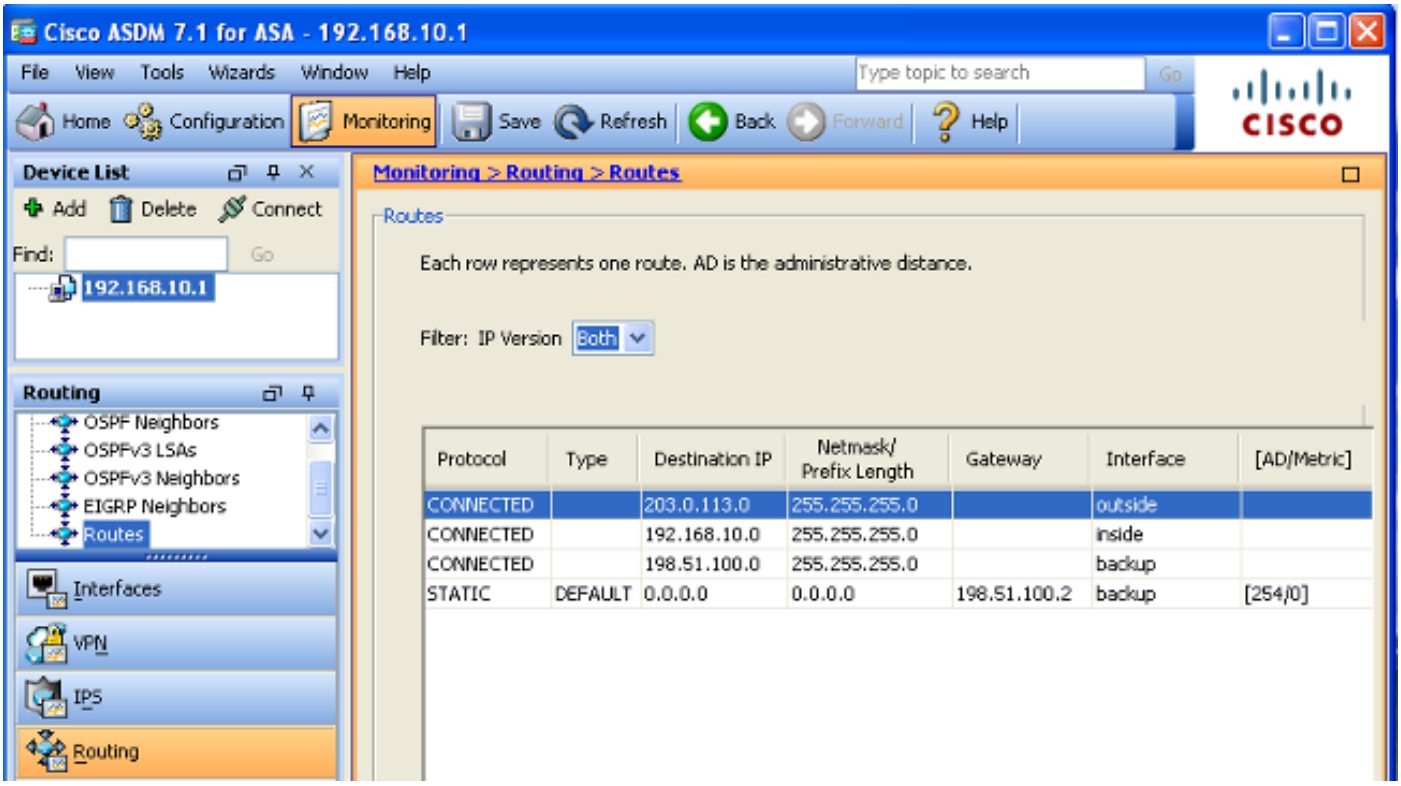
Подтвердите, что Резервный маршрут Установлен (Метод ASDM)

Чтобы подтвердить, что резервный маршрут установлен через ASDM, перейдите к **Мониторингу> Маршрутизация**, и затем выберите **Routes** из Дерева маршрутизации.

Перед сбоями основного поставщика услуг Интернет таблица маршрутизации кажется подобной показанному в следующем образе. Обратите внимание на то, что **МАРШРУТ ПО УМОЛЧАНИЮ** указывает к **203.0.113.2** через **внешний интерфейс**:



После сбоя основного поставщика его маршрут удаляется и устанавливается резервный маршрут. **МАРШРУТ ПО УМОЛЧАНИЮ** теперь указывает к **198.51.100.2** через **резервный интерфейс**:



Устранение неполадок

Этот раздел предоставляет некоторые полезные команды отладки и описывает, как решить проблему, куда отслеживаемый маршрут удален излишне.

Команды "debug"

Можно использовать эти команды отладки для устранения проблем проблем конфигурации:

- **трассировка монитора SLA отладки** – выходные данные этой команды отображают выполнение операции эха.

  Если отслеживаемый объект (шлюз основного поставщика) подключен, и эхо - запрос ICMP успешно выполняются, выходные данные кажутся подобными этому:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=1 OK
IP SLA Monitor(123) Scheduler: Updating result
```

  Если отслеживаемый объект (шлюз основного поставщика) не работает и сбой эхо - запрос ICMP, выходные данные кажутся подобными этому:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```

- **ошибка монитора SLA отладки** – выходные данные этой команды отображают любые

ошибки, с которыми встречается процесс монитора SLA.

Если отслеживаемый объект (шлюз основного поставщика) подключен, и ICMP успешно выполняется, выходные данные кажутся подобными этому:

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
```

Если отслеживаемый объект (шлюз основного поставщика) не работает, и отслеживаемый маршрут удален, выходные данные кажутся подобными этому:

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside

!--- 4.2.2.2 is unreachable, so the route to the Primary ISP is removed.
```

Ненужное удаление отслеживаемого маршрута

Если отслеживаемый маршрут удален излишне, гарантируйте, что ваша цель мониторинга всегда доступна для получения запросов эха. Кроме того, убедитесь, что состояние объекта мониторинга (т.е. достижим ли он) тесно связано с состоянием подключения к основному поставщику.

Если вы выбираете контролирующую цель, которая более далека, чем шлюз поставщика, другая ссылка вдоль того маршрута могла бы отказать, или другое устройство могло бы вмешаться. Эта конфигурация могла бы заставить монитор SLA приходить к заключению, что связь с основным поставщиком услуг Интернет прервалась и заставляет ASA излишне переключаться при отказе к вторичному каналу поставщика.

Например, если в качестве объекта мониторинга выбран маршрутизатор филиала компании, то возможен сбой подключения поставщика к этому филиалу, а также сбой

любого другого канала на всем пути. Как только эхо - запрос ICMP, которые передаются сбоем мониторинга работы, основной отслеживаемый маршрут, удалены, даже при том, что ссылка основного поставщика услуг Интернет все еще активна.

В этом примере шлюз основного поставщика, используемый как объект отслеживания, управляется поставщиком услуг Интернета и располагается на другой стороне канала поставщика. Эта конфигурация гарантирует что, если эхо - запрос ICMP, которые передаются сбоем мониторинга работы, канал поставщика, почти, конечно, не работает.

Дополнительные сведения

- Cisco ASA 5500-X Series межсетевые экраны следующего поколения
- Cisco Systems – техническая поддержка и документация