Резервирование каналов связи при помощи пакета «changeroutes»

Назначение документа

Документ описывает ряд необходимых процедур, которые нужно выполнить на С-Терра Шлюз, чтобы реализовать возможность резервирования каналов связи при помощи пакета «changeroutes».

Краткое описание пакета «changeroutes»

Пакет «changeroutes» предназначен для резервирования каналов связи (Интернет провайдеров) в режиме основной/резервный. Пакет «changeroutes» разработан для функционирования на шлюзах безопасности «С-Терра Шлюз 4.2».

Сервис `changeroutes` конфигурируется через файл `/etc/changeroutes/changeroutes.ini`.

Доступность канала определяется по доступности хостов (параметр `IP_HOSTS` в конфигурационном файле) посредством протокола ICMP – если доступен хоть один хост, указанный в `IP_HOSTS`, то канал считается рабочим. Как только все хосты становятся недоступны, то происходит переключение на резервный канал. При восстановлении основного канала происходит обратное переключение.

Ограничения и особенности пакета «changeroutes»

1) Не устанавливайте версии пакета `changeroutes` ниже чем `2.00~sterra-2` на СКЗИ КС2/КС3, так как после перезагрузки ОС Шлюз будет неработоспособен.
2) Также, если на аппаратной платформе установлен АПМДЗ, то следует пересчитать хеш суммы.

1. Максимальное количество поддерживаемых интерфейсов: 2 (active/passive).
2. Получение сетевых параметров по DHCP на отслеживаемых интерфейсах **настоятельно не рекомендуется к использованию** в текущей версии `3.02~sterra-1`.
3. Так как сервис `changeroutes` сам управляет маршрутами по умолчанию, то задавать их вручную через консоль cisco-like, либо LSP – запрещено.
4. Состояние резервного канала не отслеживается: при недоступном основном происходит безусловное переключение на резервный.
5. При переключении канала происходит очистка текущих ISAKMP/IPsec туннелей и таблицы трансляций NAT.
6. Резервирование каналов в сценарии RRI (reverse route injection) может приводить к проблемам при переключении, так как механизм RRI добавляет маршруты до защищаемых подсетей через шлюз по умолчанию.

Требования к квалификации инженера

Инженер, планирующий использовать данную инструкцию, должен свободно ориентироваться в настройке базовых сценариев продукта «С-Терра Шлюз» (например, site-to-site IPsec), а также должен знать и понимать следующие технологии и протоколы: PKI, IPsec, NAT, Firewall.

Требования к начальному состоянию «С-Терра Шлюз»

Перед настройкой должно быть выполнено следующее:

1. Шлюз должен быть инициализирован.
2. На шлюзе должны быть установлены корневой сертификат УЦ и сертификат устройства.

Исключительно для тестовых целей можно использовать тестовый УЦ от «КриптоПро», веб-интерфейс: https://www.cryptopro.ru/certsrv/certrqxt.asp.

Настройка резервирования каналов связи

Установка пакета «changeroutes»

1. Загрузите deb-пакет `changeroutes_3.02~sterra-1_all.deb` с личного кабинета Партнера (https://www.s-terra.ru/auth/).
2. Доставьте deb-пакет `changeroutes_3.02~sterra-1_all.deb` на С-Терра Шлюз и установите его:

```
root@sterragate:~# dpkg -i changeroutes_3.02~sterra-1_all.deb
```

```
Selecting previously unselected package changeroutes.
(Reading database ... 18517 files and directories currently installed.)
Unpacking changeroutes (from changeroutes_3.02~sterra-1_all.deb) ...
Setting up changeroutes (3.02~sterra-1) ...
```

После установки deb-пакета конфигурационный файл `changeroutes.ini` будет располагаться в директории `/etc/changeroutes`.

Общий алгоритм настройки сервиса changeroutes

При конфигурировании сервиса `changeroutes` нужно **обязательно** соблюдать следующие правила:
1) Все параметры должны быть представлены в конфигурационном файле.
2) Значения всех параметров должны быть указаны в двойных кавычках.
3) Нельзя использовать пробелы между параметром, знаком равно и значением параметра (только так: `MAIN_INTERFACE="eth0"` и никак иначе).
4) Строки с параметрами не должны содержать пробелов ни в начале, ни в конце.
5) Нельзя использовать комментарий на той же строке, где задан параметр.
6) Если используется несколько IP хостов для определения доступности канала, то IP-адреса должны быть разделены пробелом (`IP_HOSTS="1.1.1.1 8.8.8.8"`).

1. Определите IP-адреса хостов по доступности которых будет определяться доступность канала и укажите их (**важно:** доступность хостов проверяется только через основной канал):

```
IP_HOSTS="1.1.1.1 8.8.8.8"
```

2. Укажите имена сетевых интерфейсов в linux нотации для основного и резервного каналов (чтобы посмотреть имена интерфейсов воспользуйтесь командой `ip address show` в Linux bash):

```
MAIN_INTERFACE="eth0"
BACKUP_INTERFACE="eth1"
```

3. Укажите адреса шлюзов по умолчанию для основного и резервного каналов:

```
MAIN_GATEWAY="172.16.15.1"
BACKUP_GATEWAY="172.16.16.1"
```

4. Запустите сервис `changeroutes` и добавьте его автозагрузку:

```
root@sterragate:~# service changeroutes start
Starting daemon changeroutes_daemon ...done.
root@sterragate:~# update-rc.d changeroutes enable
```

Посмотреть лог работы сервиса можно в файле `/var/log/cspvpngate.log`:

```
root@sterragate:~# tail -n 1000 /var/log/cspvpngate.log | grep changeroutes
Sep  7 19:10:36 sterragate changeroutes: INFO: service was started with
parameters:  IP_HOSTS=1.1.1.1 8.8.8.8, MAIN_INTERFACE=eth0,
BACKUP_INTERFACE=eth1, MAIN_GATEWAY=172.16.15.1, BACKUP_GATEWAY=172.16.16.1,
FAILURE_PING_COUNT=10, PING_INTERVAL=3, RESTORE_PING_COUNT=10,
RESTORE_PING_INTERVAL=1.
Sep  7 19:10:36 sterragate changeroutes: INFO: all ISAKMP/IPsec SA was deleted.
Sep  7 19:10:36 sterragate changeroutes: INFO: all NAT translations was deleted.
Sep  7 19:10:36 sterragate changeroutes: INFO: switch to main interface eth0.
```

Общий алгоритм настройки защищенных IPsec соединений

Перед началом настройки IKE/IPsec шлюз должен быть инициализирован, должны быть выпущены и установлены сертификаты.

1. Параметры IKE/IPsec (предположим, что шлюз на котором настраивается резервирование каналов, защищает взаимодействие между локальной подсетью 192.168.20.0/24 и удаленной 192.168.1.0/24; и имеет внешний IP-адрес 172.16.15.2 на основном канале и 172.16.16.2 – на резервном):

Количество крипто-карт должно соответствовать количеству внешних интерфейсов (отличие между крипто-картами должно быть только в значении параметра `local-address`).
Параметр `local-address` нужно использовать **обязательно**.

```
crypto ipsec df-bit clear
crypto isakmp identity dn
crypto isakmp session-time-max 10
crypto isakmp keepalive 1 3
crypto isakmp keepalive retry-count 3
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto ipsec transform-set GOST esp-gost28147-4m-imit
!
ip access-list extended hub_spoke
 permit ip 192.168.20.0 0.0.0.255 192.168.1.0 0.0.0.255
!
crypto map ISP1 1 ipsec-isakmp
 match address hub_spoke
 set transform-set GOST
 set dead-connection history off
 set local-address 172.16.15.2
 set peer 172.16.10.2
!
crypto map ISP2 1 ipsec-isakmp
 match address hub_spoke
```

```
 set transform-set GOST
 set dead-connection history off
 set local-address 172.16.16.2
 set peer 172.16.10.2
!
```

2. Параметры межсетевого экрана и рекомендации при использовании NAT:

Основная идея списков доступа в данном контексте – исключение ассиметричной маршрутизации (блокировка IKE/IPsec соединений на резервном канале, если доступен основной).

```
ip access-list extended DROP_IKE_FROM_GI1/1
 deny   udp host 172.16.15.2 eq isakmp any
 deny   udp host 172.16.15.2 eq non500-isakmp any
 permit ip any any
!
ip access-list extended DROP_IKE_FROM_GI1/2
 deny   udp host 172.16.16.2 eq isakmp any
 deny   udp host 172.16.16.2 eq non500-isakmp any
 permit ip any any
```

Список доступа `DROP_IKE_FROM_GI1/2` будет использоваться для блокировки на интерфейсе `GigabitEthernet1/1` исходящих IKE/NAT-T пакетов, которые имеют IP-адрес источника, принадлежащий к интерфейсу `GigabitEthernet1/2` (для `DROP_IKE_FROM_GI1/1` аналогично).
ВАЖНО: если на шлюзе используется source NAT (обязательно ознакомьтесь с документом «Использование утилиты «iptables»), то его нужно настраивать так, чтобы локальные IKE пакеты не попадали под его правила, также не забывайте исключать защищаемые подсети из source NAT (так как source NAT происходит до зашифрования), например:

```
####### Для трафика через основной канал #######
# Исключение из правил NAT локальных IKE пакетов.
iptables -t nat -A POSTROUTING -o eth0 -s 172.16.15.2 -p udp --source-port 500 -
j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -s 172.16.15.2 -p udp --source-port 4500
-j ACCEPT
# Исключение из правил NAT защищаемого трафика.
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.20.0/24 -d 192.168.1.0/24 -j
ACCEPT
# Включение source NAT для оставшегося трафика.
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.20.0/24 -j SNAT --to-source
172.16.15.2

####### Для трафика через резервный канал #######
# Исключение из правил NAT локальных IKE пакетов.
iptables -t nat -A POSTROUTING -o eth1 -s 172.16.16.2 -p udp --source-port 500 -
j ACCEPT
iptables -t nat -A POSTROUTING -o eth1 -s 172.16.16.2 -p udp --source-port 4500
-j ACCEPT
# Исключение из правил NAT защищаемого трафика.
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.20.0/24 -d 192.168.1.0/24 -j
ACCEPT
# Включение source NAT для оставшегося трафика.
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.20.0/24 -j SNAT --to-source
172.16.16.2
```

3. Прикрепление крипто-карт и списков доступа к интерфейсам:

```
interface GigabitEthernet1/1
```

```
 ip address 172.16.15.2 255.255.255.0
 ip access-group DROP_IKE_FROM_GI1/2 out
 crypto map ISP1
!
interface GigabitEthernet1/2
 ip address 172.16.16.2 255.255.255.0
 ip access-group DROP_IKE_FROM_GI1/1 out
 crypto map ISP2
```