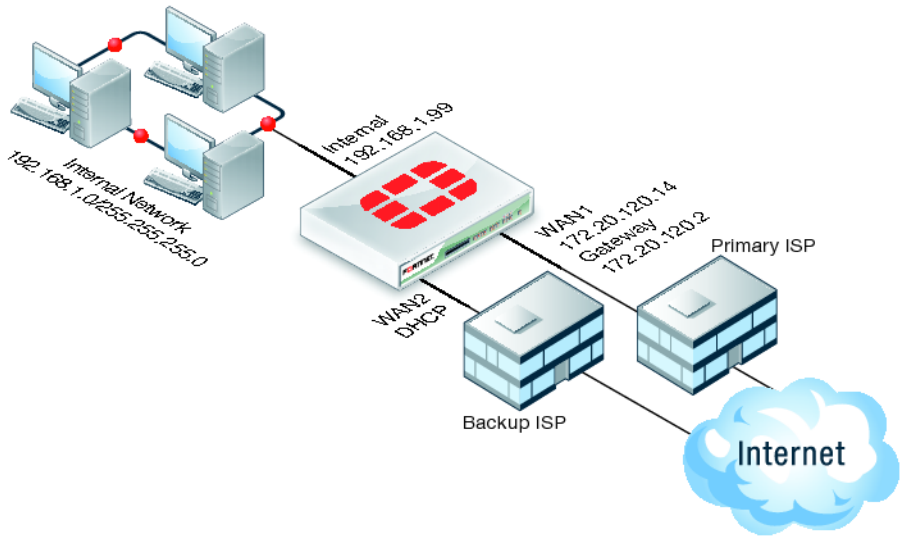
Подключение межсетевого экрана Fortigate к двум интернет провайдерам для обеспечения отказоустойчивого подключения к Интернет

Задача
Подключить резервное Интернет соединение к устройству FortiGate, таким образом чтобы в момент выхода из строя основного Интернет подключения, часть либо весь трафик автоматически переключается на резервное Интернет подключение. Как только основное Интернет подключение восстановлено, трафик автоматически должен переключиться на основной канал.



Решение
Видео: http://docs.fortinet.com/cb/inst2.html

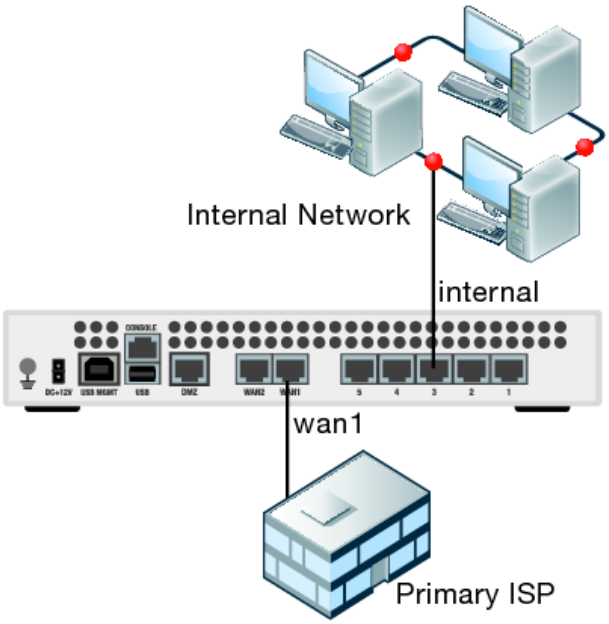
Ниже описана процедура настройки отказоустойчивого подключения с использованием двух интернет каналов. В решении основной канал подключен к интерфейсу **wan1** устройства с использованием статического IP адреса. Резервный канал подключен в интерфейсу **wan2**, IP адрес которого назначается по протоколу DHCP.

Для того чтобы разрешить прохождение трафика из сети internal через интерфейс wan1, необходимо создать политику безопасности. Также необходимо создать дополнительную политику безопасности для прохождения трафика из сети internal через интерфейс wan2.

Примечание: можно значительно сократить объемы трафика по резервирующему wan2 интерфейсу используя ограничение полосы пропускания и веб-фильтрацию FortiGuard для не приоритетных веб- сайтов. Также можно использовать функцию контроля приложений для установки ограничений использования резервного интерфейса.

Настройка основного Интернет подключения (интерфейс wan1).

1. Подключите интерфейс **wan1** устройства к оборудованию основного интернет провайдера. Подключите внутреннюю сеть к интерфейсу internal.



2. Используя ПК из внутренней сети подключитесь к веб интерфейсу устройства (IP адрес по умолчанию 192.168.1.99) используя логин **admin** без пароля.
3. Зайдите в меню **System->Network->Interface->Edit**, выберите интерфейс **wan1** и измените следующие настройки:

Addressing mode	Manual
IP/Netmask	172.20.120.14/255.255.255.0

4. Зайдите в меню **System->Network->Interface->Edit**, выберите интерфейс **internal** и измените следующие настройки:

Addressing mode	Manual
IP/Netmask	192.168.1.99/255.255.255.0

5. Зайдите в меню **Router->Static->Static Route**, выберите **Create New** и добаввьте маршрут по умолчанию:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1
IP/Netmask	172.20.17.2

6. Зайдите в меню **System->Network->DNS**, добавьте DNS сервера в полях **Primary** и **Secondary.**
7. Для того чтобы добавить политику безопасности, которая разрешает пользователям внутренней сети получать доступ к сети Интернет через интерфейс wan1, зайдите в меню **Policy->Policy**, выберите пункт **Create New->Policy**

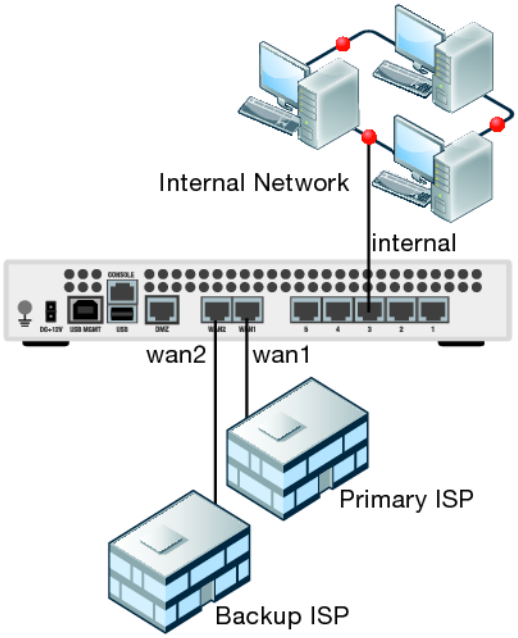
Примечание: в некоторых моделях FortiGate данная политика присутствует в заводской конфигурации. Если политика присутствует, пропустите этот пункт

Source interface/Zone	Internal
Source address	All
Destination Interface/Zone	wan1
Destination Address	All
Schedule	always
Service	ANY
Action	ACCEPT

8. Включите **Enable NAT** и **Use Destination Interface Address**
9. Для сохранения настроек нажмите кнопку **OK**

Настройка резервного Интернет подключения через интерфейс wan2

1. Подключите интерфейс wan2 устройства к оборудованию резервного интернет провайдера.



2. Подключитесь к веб-интерфейсу устройства.
3. Зайдите в меню **System -> Network -> Interface->Edit**, выберите интерфейс **wan2**.
4. Установите параметр **Addressing Mode->DHCP** и выберите параметр **Retrieve Default Gateway.** Отключите параметр **Override Internal DNS.**
5. Для сохранения настроек нажмите кнопку **OK**

   Если физическое подключение сделано правильно, на интерфейс wan2 должен быть назначен IP адрес от DHCP сервера. Данная операция может занять несколько минут. Для проверки состояния воспользуйтесь ссылкой **Status**. Полученный адрес должен появиться в статусной строке **Obtained IP/Netmask.** Если DHCP сервер передает адреса DNS серверов, они также должны появиться в статусной строке.

Внимание!: *убедитесь что параметр* ***Retrieve Default Gateway from server*** *активирован и маршрут по умолчанию появился в таблице маршрутизации. Обычно в резервируемых конфигурациях должен быть включен параметр* ***Override Internal DNS****, поскольку нет необходимости использовать DNS сервера резервного интернет провайдера*

6. Для того чтобы добавить политику безопасности, которая разрешает пользователям внутренней сети получить доступ к сети Интернет через интерфейс wan2, зайдите в меню **Policy->Policy** , выберите пункт **Create New->Policy**

Source interface/Zone	Internal
Source address	All
Destination	wan2

Interface/Zone	
Destination Address	All
Schedule	always
Service	ANY
Action	ACCEPT

7. Включите **Enable NAT** и **Use Destination Interface Address**.
8. Для сохранения настроек нажмите кнопку **OK**

Настройка шлюза по умолчанию через интерфейс wan1 как приоритетный маршрут, а также настройка ping серверов для интерфейсов wan1 и wan2

На устройстве FortiGate должны быть настроены два маршрута по умолчанию, один направляет трафик через интерфейс wan1, второй, через интерфейс wan2.

Примечание: поскольку маршрут по умолчанию для интерфейса wan2 устройство получает от интернет провайдера по протоколу DHCP, необходимо отредактировать интерфейс wan2 и изменить дистанцию для маршрута.

1. Зайдите в меню **Router->Static->Static Route.** Отредактируйте(**Edit**) маршрут по умолчанию для интерфейса wan1, выберите пункт **Advanced** и установите значение параметра **Distance** в **10**.
2. Зайдите в меню **System->Network->Interface.** Отредактируйте интерфейс **wlan2** и установите параметр **Distance** в **20** (либо любое другое значение больше 10).
3. Используйте функции мониторинга меню **Router->Monitor->Routing Monitor** для проверки какой маршрут по умолчанию используется. Неиспользуемые маршруты не появляются в таблице маршрутизации. В примере ниже виден только статический маршрут(дистанция 10) через интерфейс wan1.

Type: All Network: Gateway:

Type	Subtype	Network	Distance	Metric	Gateway	Interface
Static		0.0.0.0/0	10	0	172.20.120.2	wan1
Connected		10.41.101.0/24	0	0	0.0.0.0	wan2
Connected		172.20.120.0/24	0	0	0.0.0.0	wan1
Connected		192.168.1.0/24	0	0	0.0.0.0	internal

Примечание: если установить на интерфейсе wan2 меньшую дистанцию (например 5), шлюз по умолчанию интерфейса wan1 будет удален , а в списке появится шлюз по умолчанию интерфейса wan2. Также можно использовать одинаковую дистанцию для обоих маршрутов по умолчанию(например 10). В таком случае будут использоваться оба маршрута по алгоритму маршрутизации множественных путей(ECMP). Активные сессии будут балансироваться по обоим интерфейсам.

4. Зайдите в меню **Router->Static->Settings->Create New**, добавьте ping сервер для интерфейса **wan1**:

Interface	wan1
Ping Server	172.20.120.2
Detect Protocol	ICMP Ping
Ping interval(seconds)	5
Failover thershold	5

5. Выберите **Create New** и добавьте ping сервер для интерфейса **wan2**.

Interface	wan2
Ping Server	10.41.101.100
Detect Protocol	ICMP Ping
Ping interval(seconds)	5
Failover thershold	5

Результаты

Если IP адрес ping сервера wan1 доступен, то в мониторе маршрутов будет доступен маршрут по умолчанию интерфейса wan1. Весь трафик маршрутизируется в Интернет через интерфейс wan1. Для проверки можно использовать монитор маршрутов либо с помощью счетчика **Count** политик **internal->wan1** и **internal->wan2** в меню **Policy->Policy.** Счетчик политики **internal->wan1** должен расти. Счетчик политики **internal->wan2** не будет изменяться.

Если ping сервер wan1 перестал быть доступным, (это можно проверить физически отключив кабель из интерфейса wan1), маршрут по умолчанию должен измениться на интерфейс wan2:

Type: All Network: Gateway:

Type	Subtype	Network	Distance	Metric	Gateway	Interface
Static		0.0.0.0/0	20	0	10.41.101.100	wan2
Connected		10.41.101.0/24	0	0	0.0.0.0	wan2
Connected		172.20.120.0/24	0	0	0.0.0.0	wan1
Connected		192.168.1.0/24	0	0	0.0.0.0	internal

Данное событие должно быть отображено в отчете событий:

```
2011-08-24 10:16:39 log_id=0100020001 type=event subtype=system
pri=critical vd=root interface="wan1" status=down msg="Ping peer:
(172.20.120.14->172.20.120.2 ping-down)"
```

Попробуйте подключиться к какому либо Интернет ресурсу, в тот момент когда соединение wan2 активно. Если вы можете подключиться, это является

подтверждением того что устройство настроено правильно. Проверьте счетчик политики безопасности **internal->wan2**. Значения счетчика должны возрастать.

Восстановите wan1 соединение. Ping сервер должен определить, что основное Интернет соединение восстановлено и изменит маршрут по умолчанию на wan1. Все новые сессии будут маршрутизироваться через это соединение. Текущие сессии, пока не будут завершены, продолжат работать через интерфейс wan2.

Примечание: во время переключения на резервное соединение, входящие сессии полученные VIP политикой безопасности с интерфейса wan1 до переключения будут быть пересланы через интерфейс wan2 после переключения. Исходящие сессии инициированные сервером через VIP политику безопасности будут иметь исходящий IP адрес того интерфейса, который на данный момент является активным.

Включение ECMP на резервном Интернет соединении

Сценарий описанный выше должен успешно работать для большинства сетей. Однако во избежание ложных срабатываний переключения (например в моменты кратковременных обрывов связи) рекомендуется активировать алгоритм ECMP. Для реализации ECMP конфигурации необходимо настроить одинаковую дистанцию на обоих соединениях и указать приоритет маршрутов. Маршрут который имеет приоритет ниже является лучшим.

Измените конфигурацию следующим образом:

1. Зайдите в меню **Router->Static->Static Route**, выберите **Edit** для маршрута wan1.
2. Выберите пункт **Advanced** и установите параметры **Distance** в **10**, **Priority** в **5**.
3. Используя интерфейс командной строки(CLI) измените дистанцию и приоритет для интерфейса wan2:

```
config system interface
   edit wan2
      set distance 10
      set priority 20
  end
```

Имея самый низкий приоритет интерфейс wan1 определяется как основной нмаршрут и весь трафик из приватной сети маршрутизируется через интерфейс wan1.

Примечание: если в маршрутах wan1 и wan2 настроены разные дистанции, ответы на входящий Интернет трафик может присылать только интерфейс с меньшей дистанцией(wan1). Если входящее соединение установлено через интерфейс wan1, оно будет разорвано в момент отказа. После кратковременного прерывания соединение будет автоматически восстановлено через интерфейс wan2. Соединение будет разорвано второй раз, как только wan1 соединение будет восстановлено, поскольку после переключения на основной канал прохождение трафика через интерфейс wan2 будет невозможно.

Если алгоритм ECMP активирован, оба интерфейса будут всегда активны. Соединение будет разорвано если произошел сбой соединения wan1, но после восстановления

работоспособности будет продолжать работать через интерфейс wan2. Таким образом разрыв соединения произойдет только один раз.