Настройка failover конфигурации и использование PBR для направления различных типов трафика через разных ISP, особенности использования SAT на двух ISP.

Будем рассматривать пример на основе следующих данных:

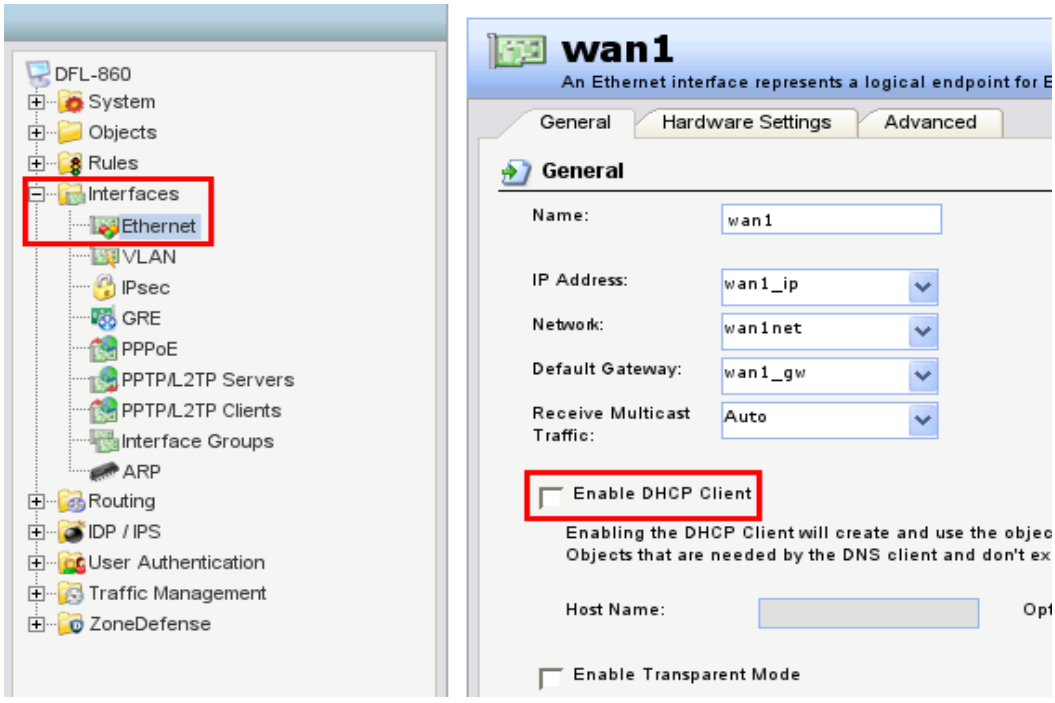
Первый ISP:
Тип подключения Статический IP
IP 192.168.60.5
Маска 255.255.255.248 (в битном виде для исходных данных 192.168.60.0/29)
Шлюз 192.168.60.1
DNS 192.168.100.1

Второй ISP
Тип подключения: Статический IP
IP 10.10.10.50
Маска 255.255.255.252 (в битном виде для исходных данных 10.10.10.48/30)
Шлюз 10.10.10.49
DNS 10.1.10.1

Установим на устройстве предоставленные провайдерами данные.

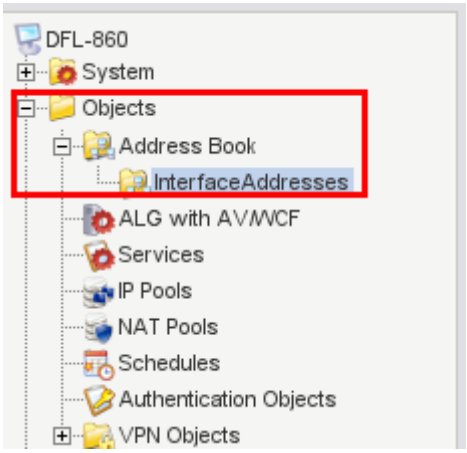
Зайдите на Web интерфейс устройства набрав в строке браузера (IE6/7 Firefox, mozilla) https://192.168.1.1, авторизируемся в появившемся окне, по умолчанию Username admin Password admin

Выберите слева Interfaces, затем Ethernet, далее wan1, снимите галочку с Enable DHCP Client и нажмите Ок.

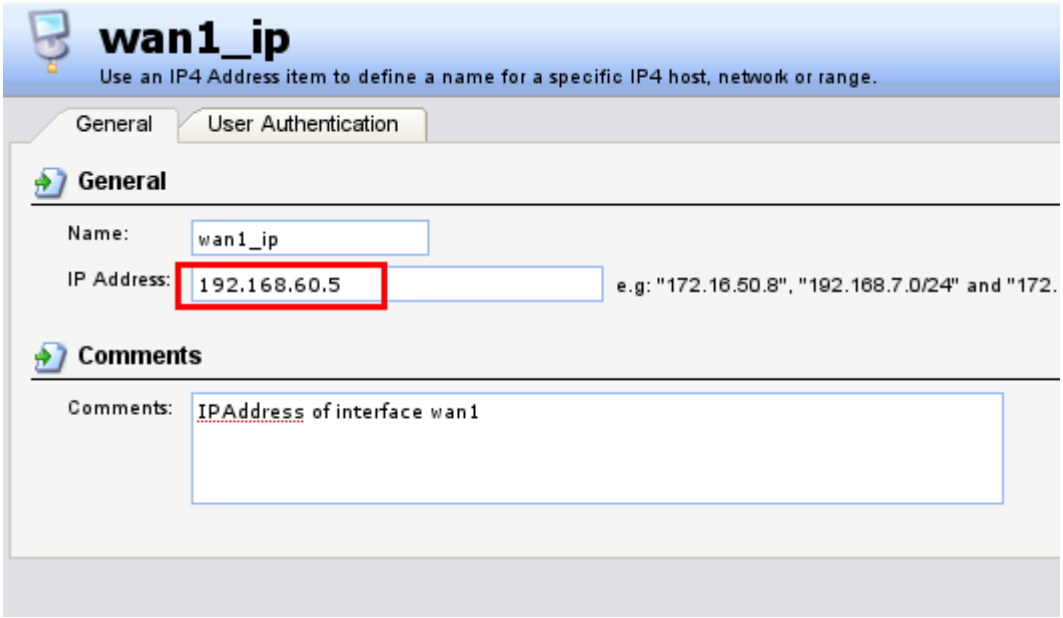


Установим данные провайдером на интерфейсы wan1 и wan2

Выберите слева Objects → Address Book → InterfaceAddresses,

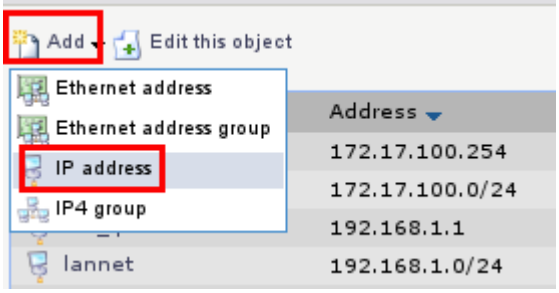


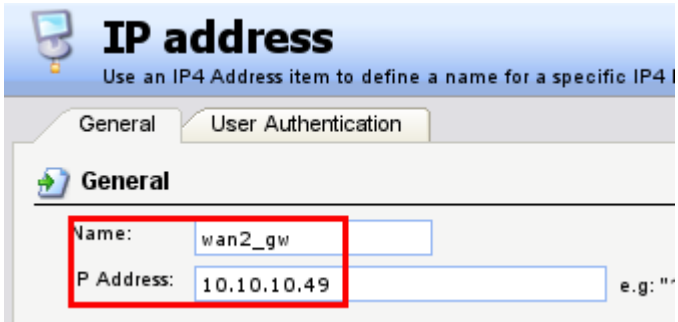
измените следующий объект, кликните на объект wan1_ip, в поле IP Address: установите 192.168.60.5 и нажмите Ок



Повторите действия с указанными объектами и выставите приведенные параметры в wan1_gw 192.168.60.1, в wan1net 192.168.60.0/29, wan1_dns1 192.168.100.1, в wan2_ip 10.10.10.50, в wan2net10.10.10.48/30.

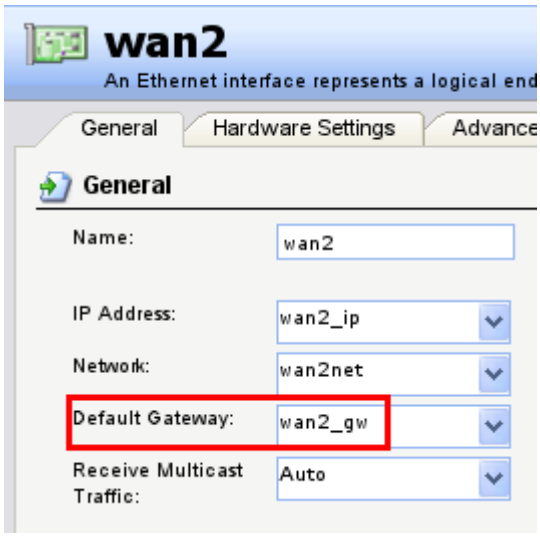
Создадим объект wan2_gw. Кликните на кнопку add из меню выберите IP addresses, в поле Name укажите wan2_gw, а в поле IP addresses 10.10.10.49, затем нажмите Ок.





Выставим шлюз на для интерфейса wan2.

Выберите слева Interfaces, затем Ethernet, далее wan2, в поле Default Gateway: выберите wan2_gw и нажмите Ок.



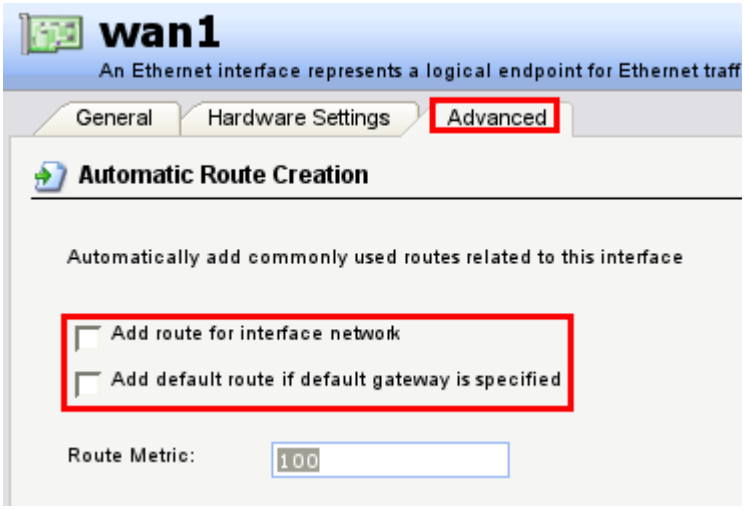
Перед настройкой Failover конфигурации акцентирую ваше внимание на особенностях данной конфигурации, прежде всего стоит обратить внимание на то, что мы разделяем маршруты к all-nents по метрике, у основного подключения метрика выставляется главнее чем на подключении которое будет использоваться как резервное (чем параметр метрики меньше тем маршрут главнее), из-за этой особенности и не работает перенаправление портов с резервного подключения, как разрешить эту ситуацию будет описано далее.

Исходим из данных, что подключение к первому ISP основное а ко второму ISP резервное.

Для переключения с основного канала на резервный необходимо отслеживать статус подключения. Устройство умеет отслеживать следующие параметры, наличие физического подключения (link) и доступность шлюза (устройство опрашивает шлюз используя ARP). Если шлюз перестанет быть доступным или пропадет физическое соединение, устройство просто отключит основной маршрут к all-nets (в нашем случае это подключение wan1), но при этом остается маршрут к all-nets на резервном подключении, через который и пойдет уже весь трафик.

Для отслеживания статуса основного соединения, надо создать два «мониторищихся» маршрута, первый wan1 - wan1net, второй wan1 — all-nets — wan1_gw и удалить существующие маршруты этого интерфейса. В первом маршруте мы будем отслеживать только наличие физического соединения (link`a) во втором наличие физического соединение и шлюза.

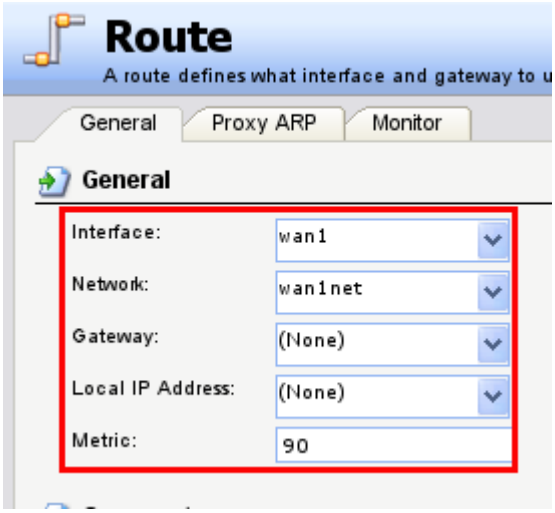
Выберите слева Interfaces → Ethernet → wan1, зайдите на вкладку Advanced и снимите галочки с Add route for interface network и Add default route if default gateway is specified и нажмите Ok.



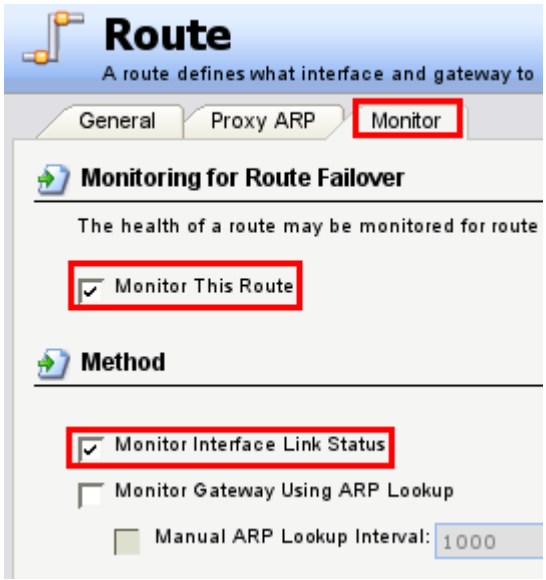
Этим действием мы удалим автоматически создающиеся маршруты на интерфейсе wan1.

Выберите слева Routing → Routing Tables → main (read-only). Вы сразу заметите два перечеркнутых маршрута, эти маршруты были созданы автоматически системой для интерфейса wan1 и будут удалены после активации настроек. Создаем два аналогичных маршрута как перечеркнутые, с другой метрикой (более главной) и активируем на этих маршрутах отслеживание статуса соединения.

Нажмите кнопку add, из выпадающего меню выберите Route, в поле Interface: укажите wan1, в поле Network: wan1net, метрику выставите 90

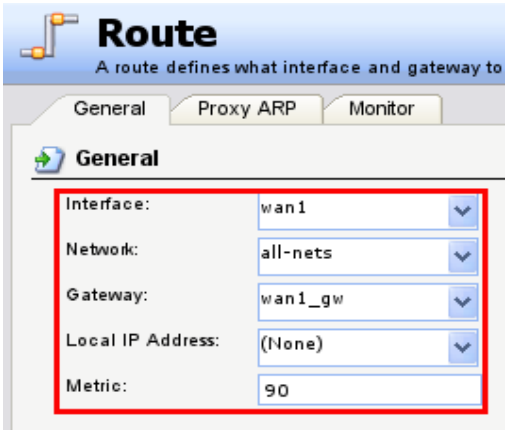


Зайдите на вкладку Monitor, установите галочки на Monitor This Route и Monitor Interface Link Status, затем нажмите Ок.

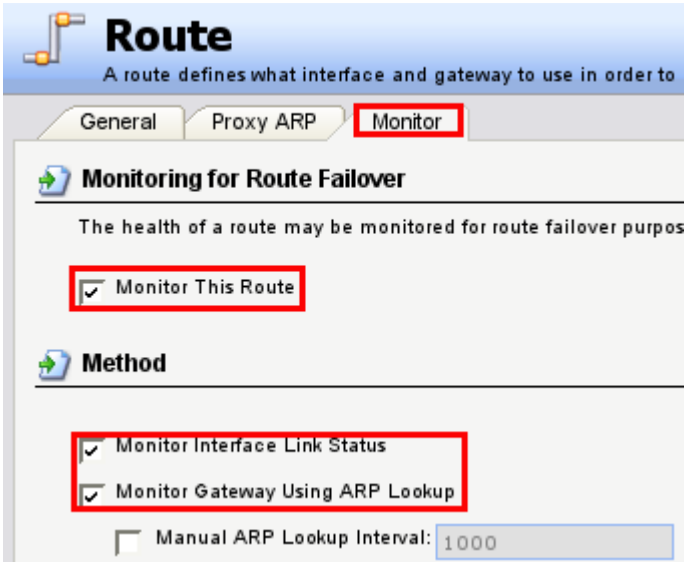


Создав этот маршрут, мы указали DFL, что на wan1 интерфейсе у него находится сеть 192.168.60.0/29, (Устройство будет обращаться к IP адресам с 192.168.60.1 по 192.168.60.6 минуя шлюз) и активировали отслеживание наличия физического соединения.

Нажмите add, из выпадающего меню выберите Route, в поле Interface: укажите wan1, в поле Network: укажите all-nets, в поле Gateway укажите wan1_gw



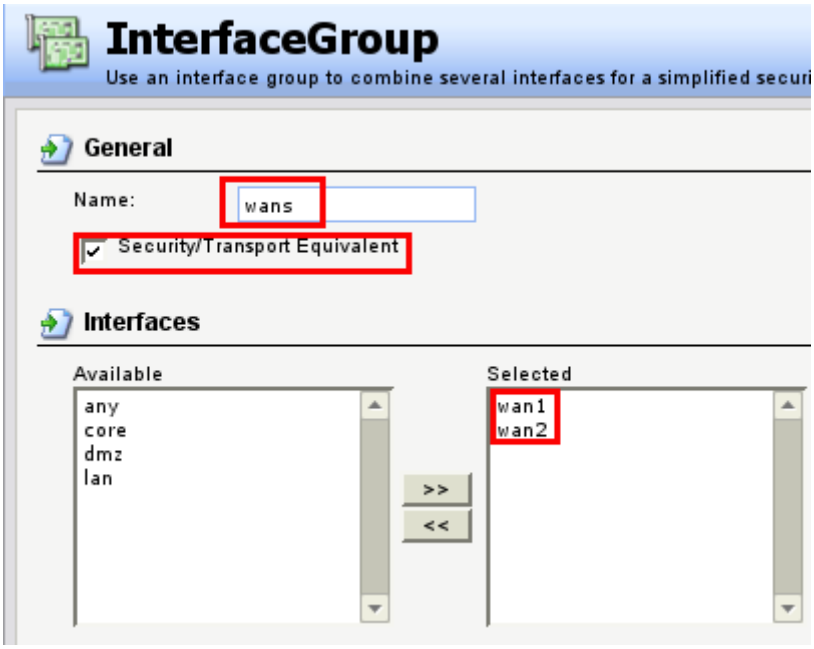
Зайдите на вкладку Monitor, установите галочки на на Monitor This Route, Monitor Interface Link Status и Monitor Gateway Using ARP Lookup, затем нажмите Ок.



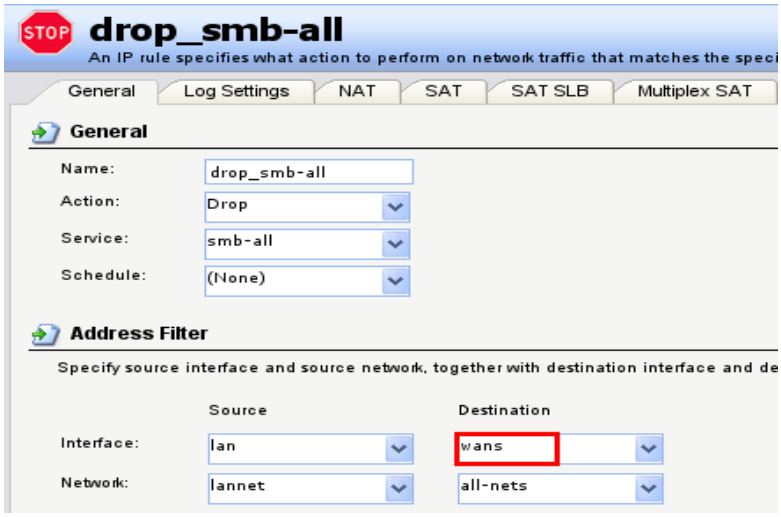
Созданием этого маршрута мы указали устройству, через wan1_gw маршрутизировать весь разрешенный трафик который предназначен для сетей не обозначенных на интерфейсах DFL и активировали отслеживание наличия физического соединения и шлюза.

Конфигурация failover готова, но еще не может полноценно использоваться, т.к. нет разрешающих правил для резервного соединения, т.е. при срабатывании failover, устройство просто не выпустит трафик через второго ISP. Изменим конфигурацию устройства для того чтоб позволить трафику проходить как через первое так и через второе подключение.

Выберите слева Interfaces → Interface Groups. Нажмите кнопку Add, выберите InterfaceGroup, в поле Name: укажите wans, теперь добавьте в группу интерфейсы wan1 и wan2 путем выделения и нажатия и нажатия кнопки > > , установите галочку Security/Transport Equivalent и нажмите Ок.



Выберите слева Rules → IP Rules → lan_to_wan1, в этой папке находятся правила управляющие доступом из сети lan в сеть wan1, изменим правила таким образом, чтоб трафик мог так же выходить и через wan2. Изменим в каждом из четырех правил интерфейс назначения с wan1 на созданную группу интерфейсов wans.



После изменения правил, они должны принять такой вид

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	drop_smb-all	Drop	lan	lannet	wans	all-nets	smb-all
2	allow_ping-outbound	NAT	lan	lannet	wans	all-nets	ping-outbound
3	allow_ftp-passthrough_av	NAT	lan	lannet	wans	all-nets	ftp-passthrough-av
4	allow_standard	NAT	lan	lannet	wans	all-nets	all_tcpudp

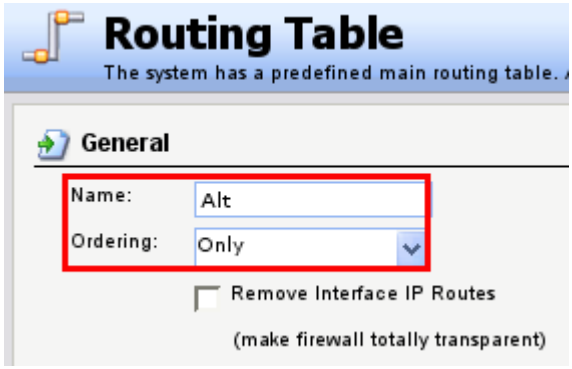
Произведенных настроек достаточно для простой failover конфигурации, можно сохранить и активировать настройки.

Настроим устройство так, чтоб оно направляло весь ftp трафик через второго провайдера, а в случае его недоступности через первого.

Перед настройкой данной конфигурации хочу акцентировать внимание на следующих особенностях, все перенаправления трафика будут осуществляться при помощи Routing Rules (PBR) которые будут просто «заворачивать» указанный трафик через альтернативную таблицу маршрутизации, в которой уже в отличии от основной таблицы маршрутизации основным подключением будет подключение через второго провайдера, а резервное через первого.

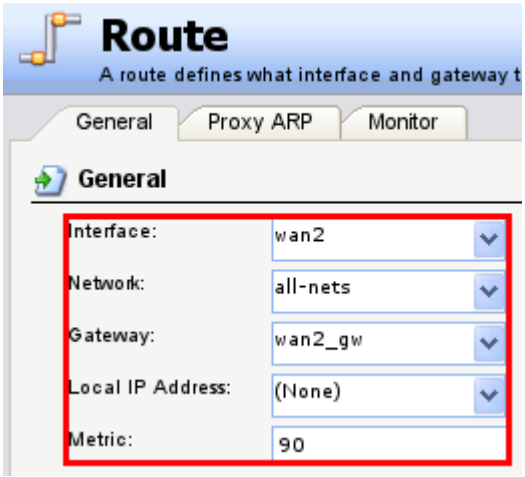
Создадим альтернативную таблицу маршрутизации и маршруты для этой таблицы.

Выберите слева Routing → Routing Tables, нажмите на кнопку Add, выберите Routing Table, в поле Name: укажите Alt, в поле Ordering выберите Only и нажмите Ok.

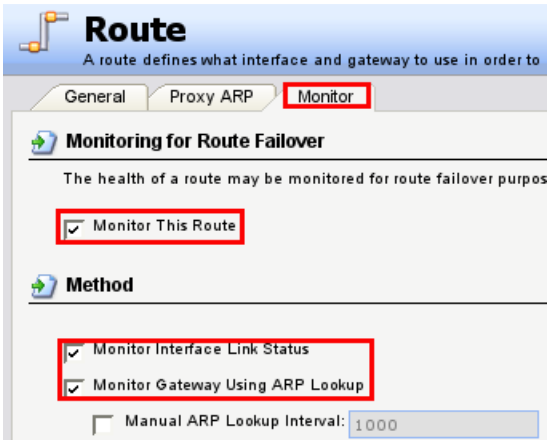


Теперь создадим основной и резервный маршрут.

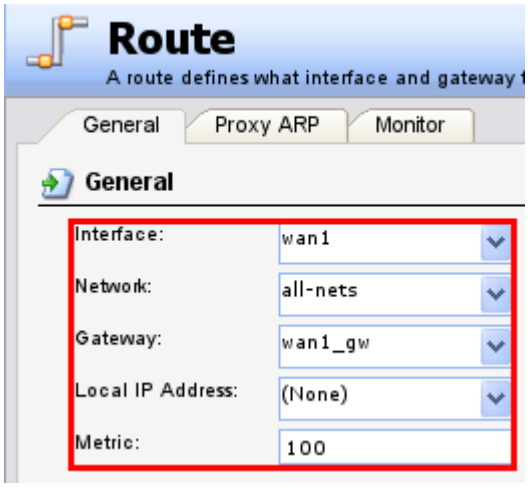
Нажмите кнопку Add, выберите из списка Route, в поле Interface укажите wan2, в поле Network: all-nets а в поле Gateway: wan2_gw, Метрику выставите 90



Зайдите на вкладку Monitor , установите галочки на на Monitor This Route, Monitor Interface Link Status и Monitor Gateway Using ARP Lookup, затем нажмите Ок.

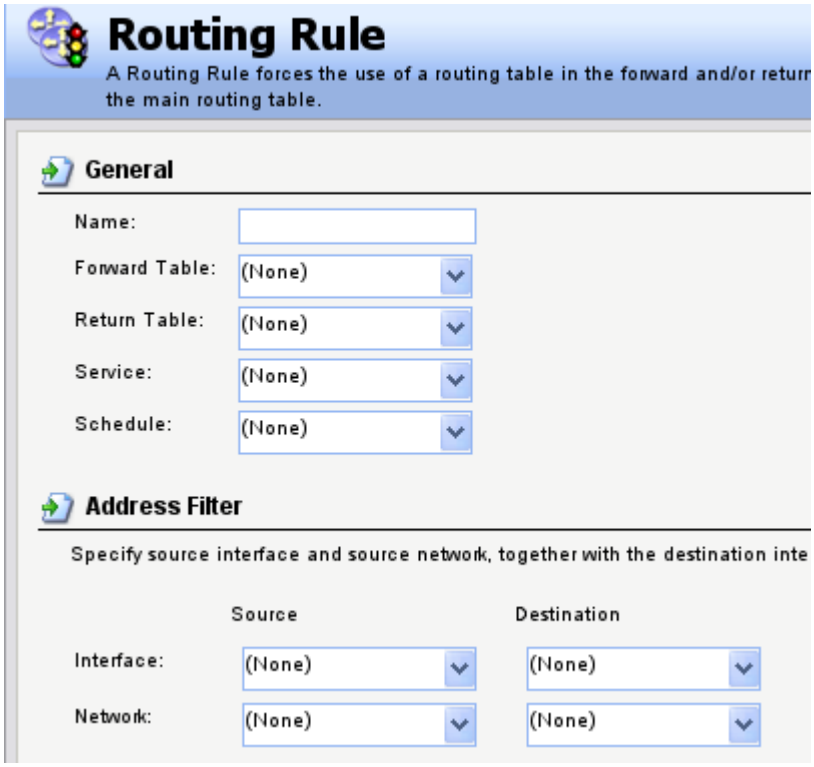


Нажмите add, из выпадающего меню выберите Route, в поле Interface: укажите wan1, в поле Network: укажите all-nets, в поле Gateway укажите wan1_gw, метрику установите 100 и нажмите Ок.



Альтернативная таблица маршрутизации готова, теперь надо при помощи PBR завернуть ftp трафик в эту таблицу.

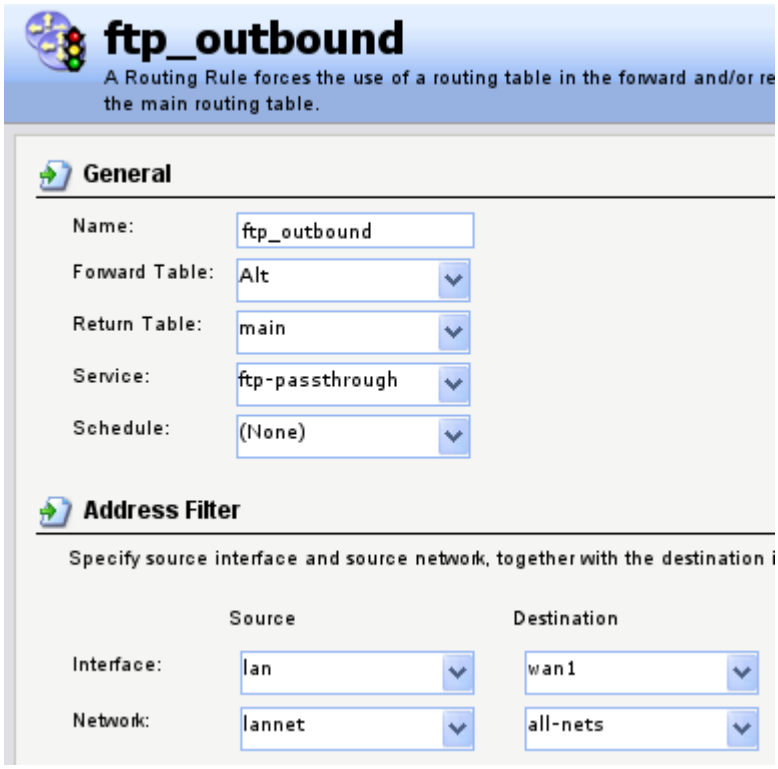
Подробнее рассмотрим Routing Rules, и логику данного правила, если понять её, то в дальнейшем вопросов как построить сложную маршрутизации с использованием PBR не возникнет.



Рассмотрим правило подробнее, в данном правиле Address Filter и Service являются фильтрами того когда это правило будет работать, а Forward Table и Return Table уже отвечают за перенаправление трафика. Forward Table указывает какую таблицу использовать для отправки трафика (исходящий трафик), а Return Table какую таблицу маршрутизации использовать для входящего трафика(входящий трафик).

Теперь создадим правило которое перенаправит ftp трафик через второго провайдера (через альтернативную таблицу маршрутизации).

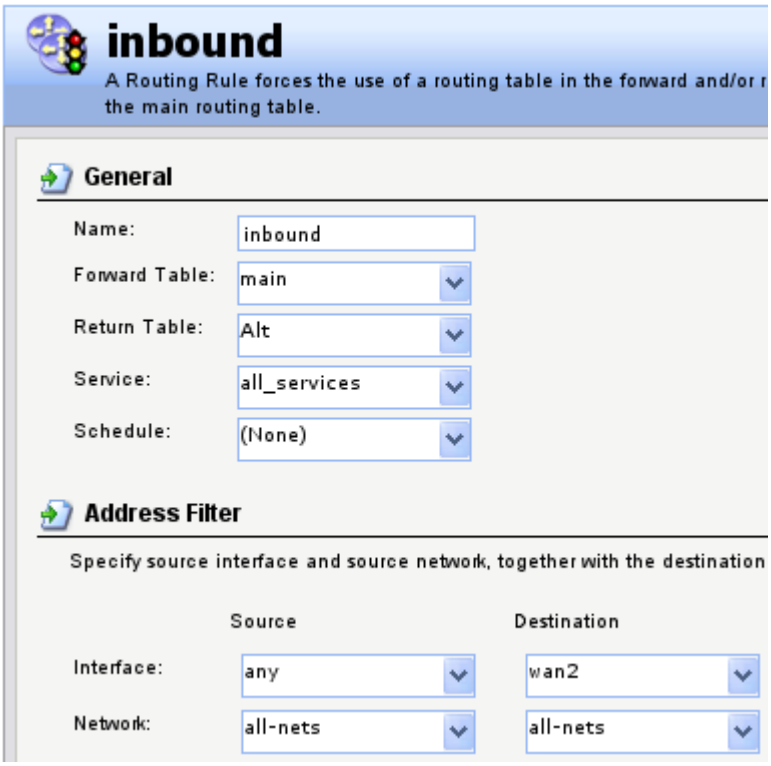
Нажмите кнопку Add, выберите Routing Rule, В поле Forward Table укажите Alt, в поле Return Table укажите main, фильтры интерфейсов хаполните следующим образом. Source Interface lan, Source Network lannet, Destination Interface wan1, Destination Network all-nets, и нажмите Ок.



Этим правилом мы указали устройству, что ftp трафик (service), направляющийся из внутренний сети lan во внешнюю сеть через первого провайдера (wan1), завернуть в альтернативную таблицу маршрутизации, где указан в качестве основного соединение wan2 (второй провайдер). В результате весь FTP трафик перенаправляется через второго провайдера. А в случае отказа второго провайдера, будет задействован уже второй маршрут в альтернативной таблице, и ftp трафик направиться уже через первого провайдера.

При необходимости можно маршрутизировать трафик только от части внутренних пользователей, просто изменив Source Network lannet на диапазон IP адресов внутренних пользователей или например маршрутизировать ftp трафик через второго провайдера в случае только когда он идет только на определенный сервер, в этом случае вместо all-nets, надо подставить IP адрес ftp сервера.

При помощи PBR, мы так же можем заставить работать проброс портов, если он используется на резервном канале, для этого надо создать правило, которое укажет устройству, что на весь входящий трафик на резервный интерфейс, отвечать с этого же интерфейса а не основного. В качестве примера смотрите скриншот подобного правила ниже.



Сохраните и активируйте настройки.