Пример настройки межсетевых экранов D-Link NetDefend

Как настроить туннель L2TP over IPSec для подключения клиентов Windows, Android, iOS.

Применимо к моделям:

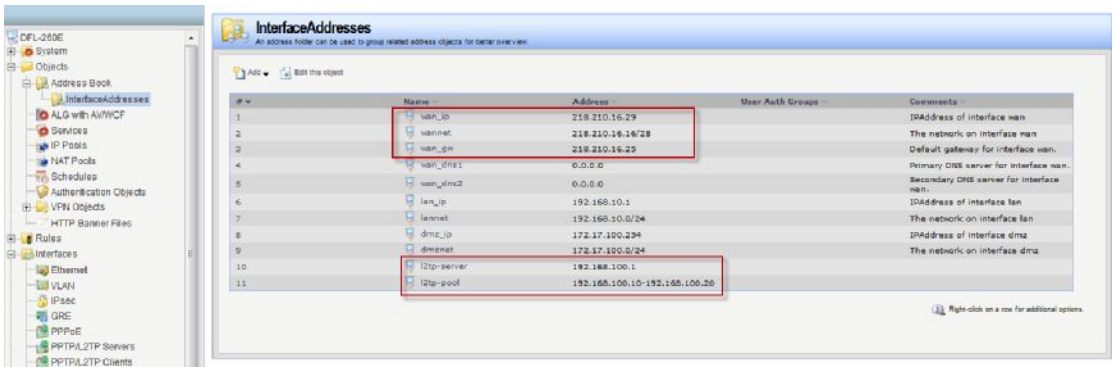
DFL-210/260/260E/800/860/860E/1600/1660/2500/2560

Топология.

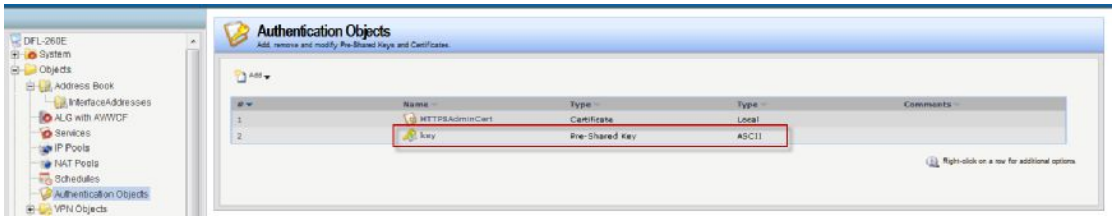
L2TP over IPsec Сервер L2TP over IPsec клиент

В данной инструкции будут указаны только те параметры, которые необходимо изменить. Остальные параметры необходимо оставить в значениях "по умолчанию".

(1) Добавляем 2 адресных объекта “l2tp-server”и “l2tp-pool”.



(2) Добавляем pre-share ключ.



Если мы хотим, что бы к нашему туннелю могли подключиться клиенты на любых операционных системах, то естественно, мы должны настроить туннель таким образом, что бы учесть особенности настройки всех этих операционных систем.

а) Особенности Windows 7 и Windows 8

Несмотря на то, что Windows 7 и Windows 8 поддерживают практически все параметры и алгоритмы IPSec, для L2TP over IPSec поддерживается всего 5

комбинаций параметров:

Proposal1	AES-256	384bit	SHA-1
Proposal2	AES-128	256bit	SHA-1
Proposal3	AES-256	Group 14 (2048bit)	SHA-1
Proposal4	3DES	Group 14 (2048bit)	SHA-1
Proposal5	3DES	Group 2 (1024bit)	SHA-1

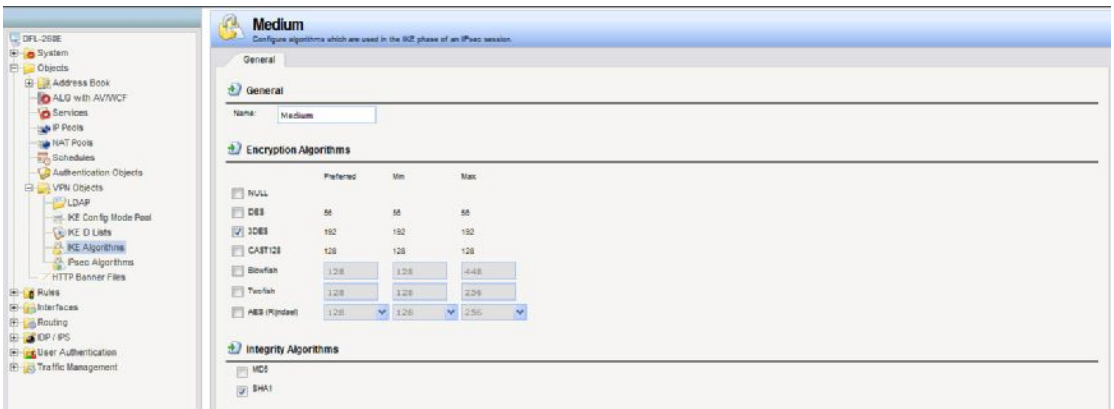
Как не трудно заметить, только Proposal5 поддерживается DFLями.

б) Особенности более ранних ОС семейства Windows
Более ранние ОС Windows не поддерживают AES и не поддерживают длину ключа DH выше 1024bit (т.е. group 5 и выше не поддерживается). Также, более ранние Windows не поддерживают: xAuth, PFS, NAT-T и DPD.

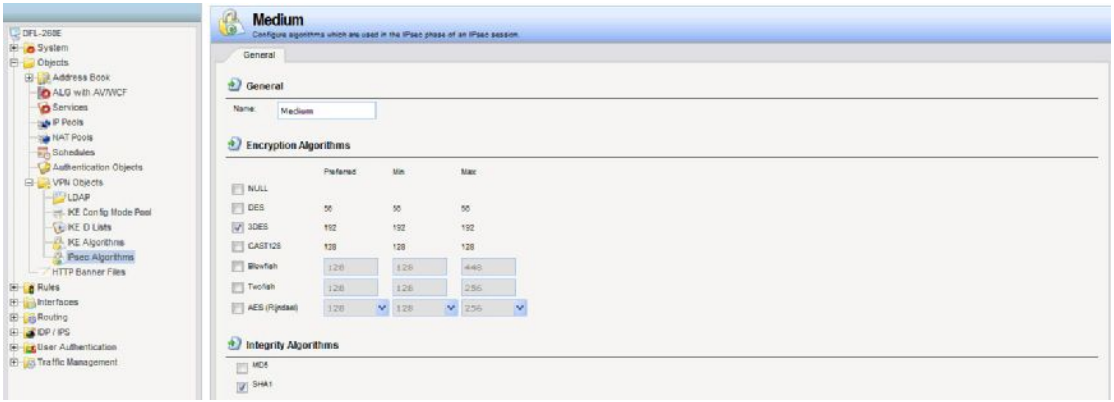
в) Особенности Андроид и iOS
Андроид и iOS (iPhonы, iPadы) не поддерживают длину ключа DH group 5 и выше, а также не поддерживают AES-192 (поддерживается только AES-128 и AES-256). Также, Андроид и iOS не поддерживают PFS.

В результате при настройке туннеля нам необходимо указать следующие параметры: шифрование - 3DES, длина ключа DH - Group 2, хеширование SHA-1. Отключить: xAuth, PFS, NAT-T и DPD.

(3) Настраиваем алгоритмы первой фазы



(4) Настраиваем алгоритмы второй фазы



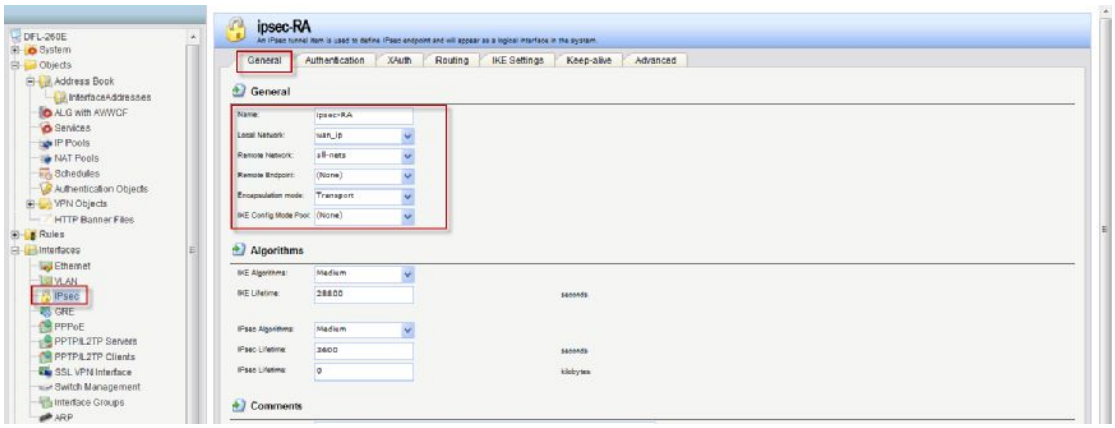
(5) Создаём IPsec туннель

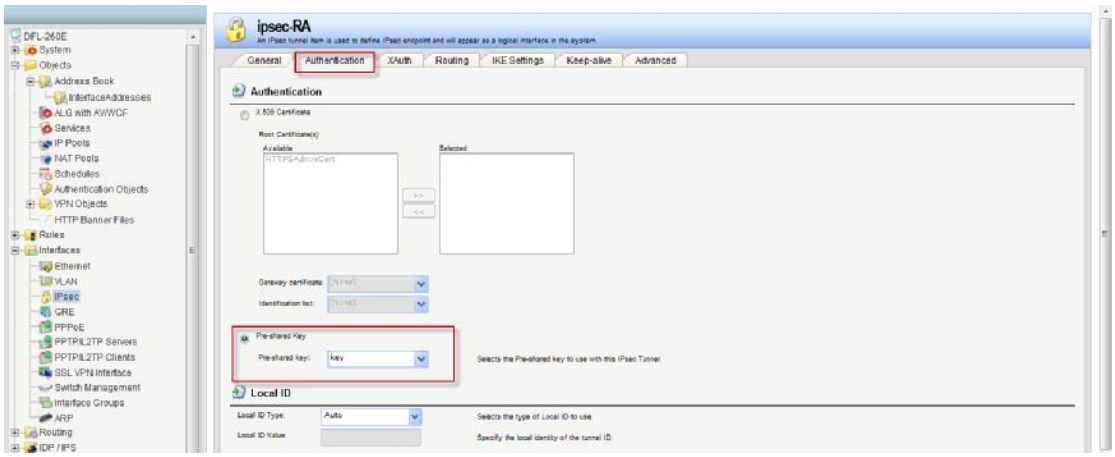
Обратите внимание на следующие параметры:

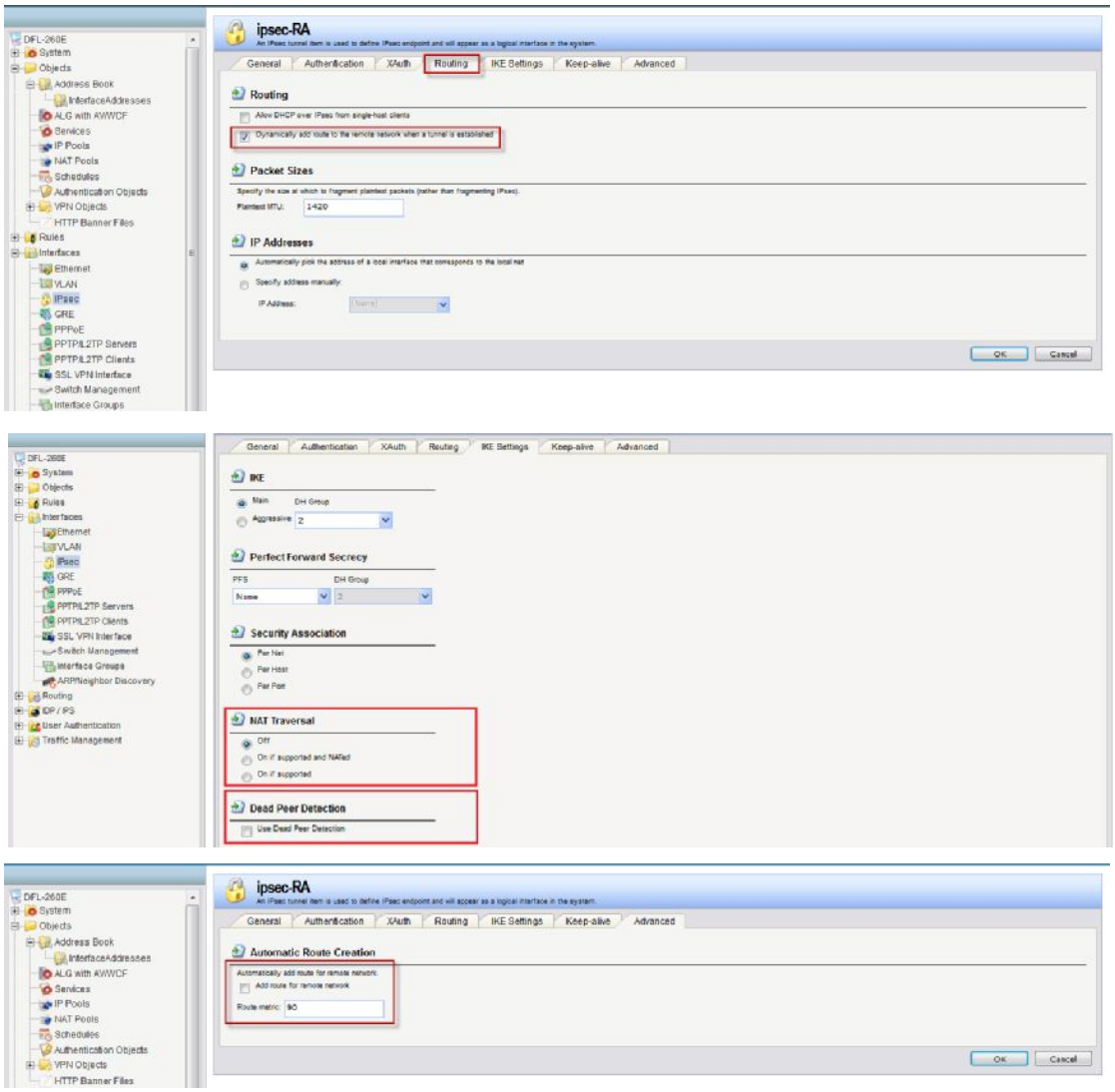
Local network “wan_ip”

Remote network “all-nets”

Encapsulation mode “Transport”







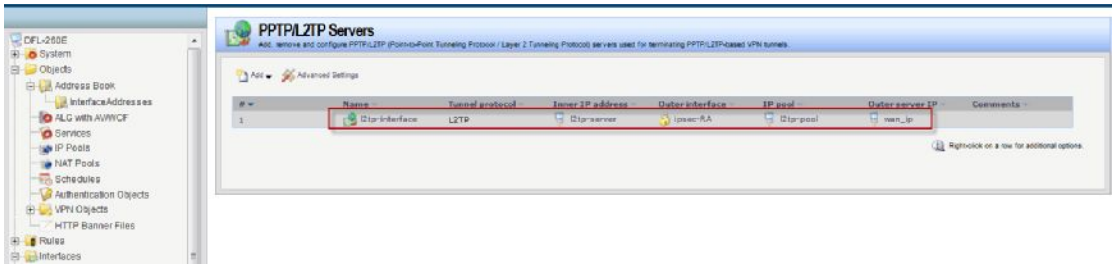
(6) Создаём L2TP сервер.

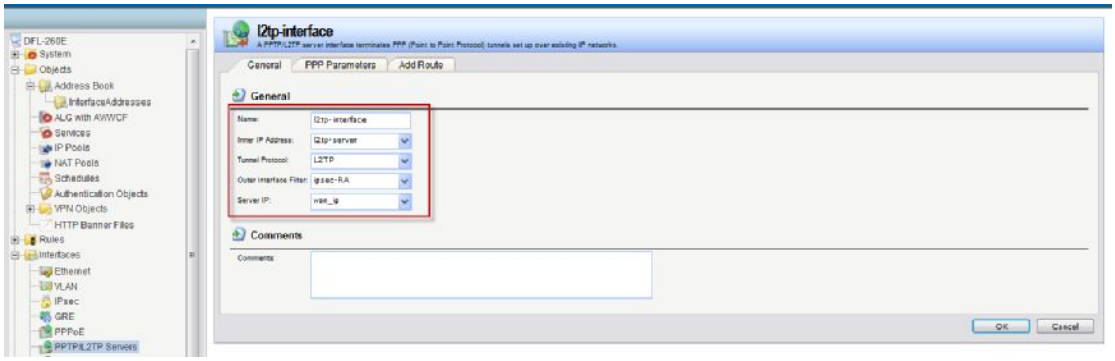
Inner IP address: “L2TP-server”

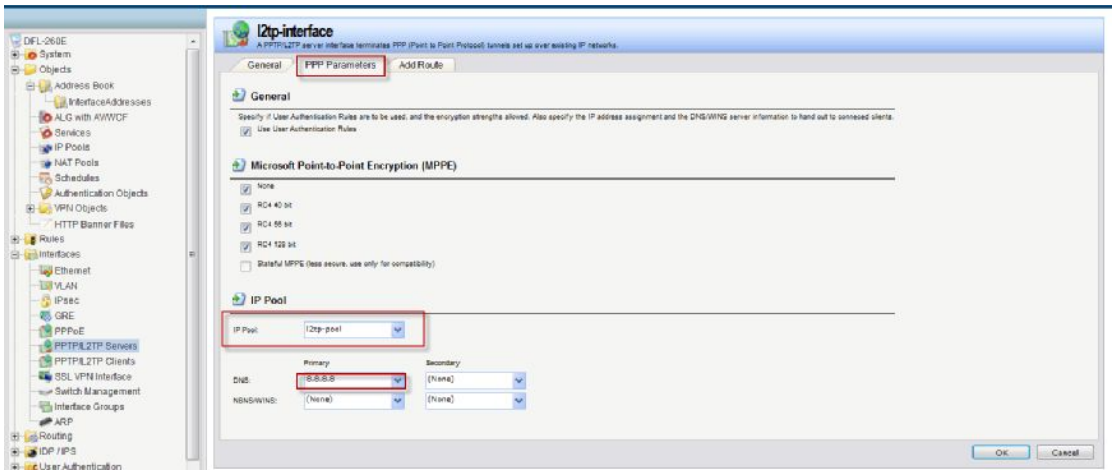
Tunnel protocol: “L2TP”

Outer interface: “IPsec-RA”

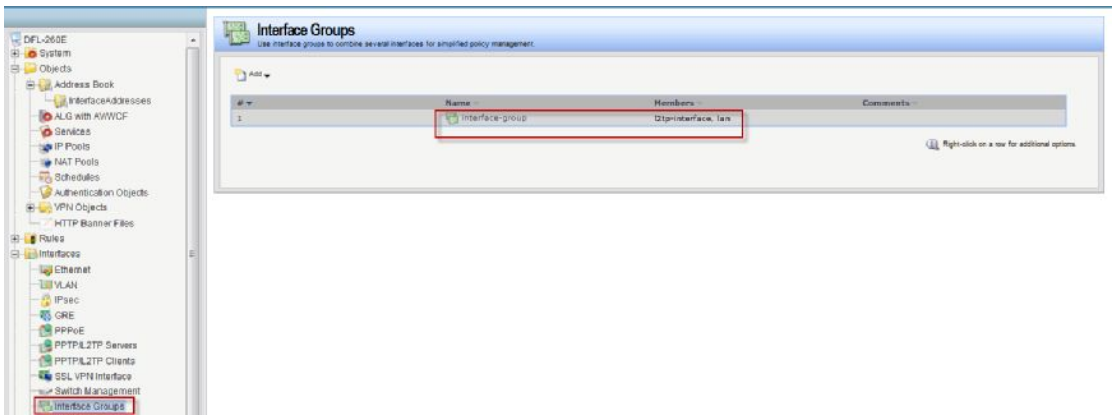
Server IP: “wan_ip”



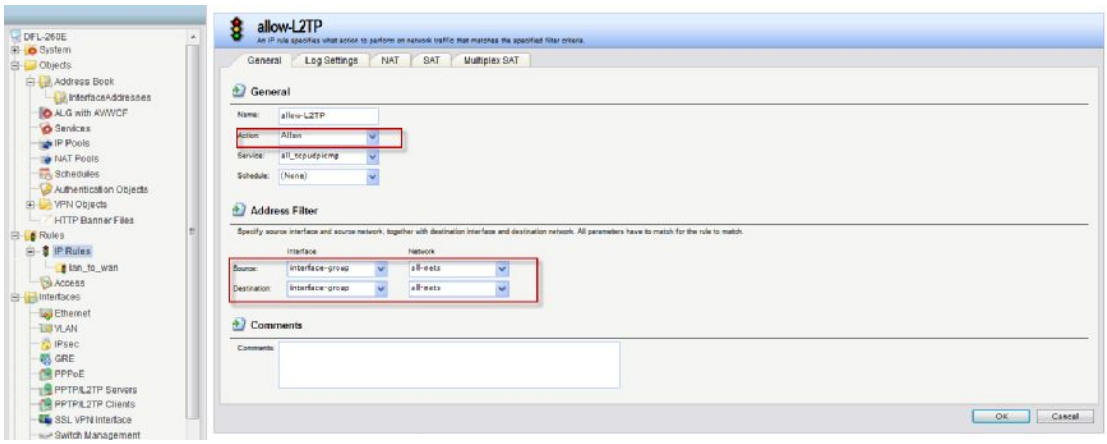




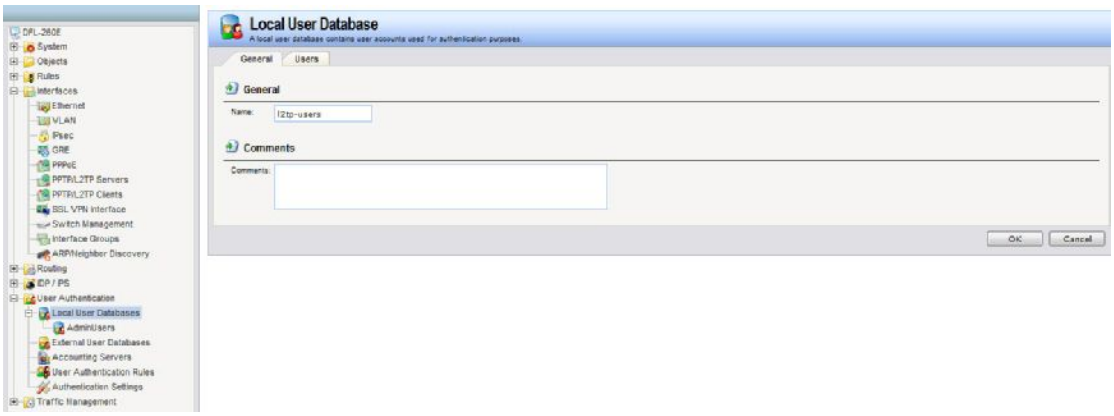
(5) Создаём новую интерфейсную группу из “L2TP-interface” и “LAN”.



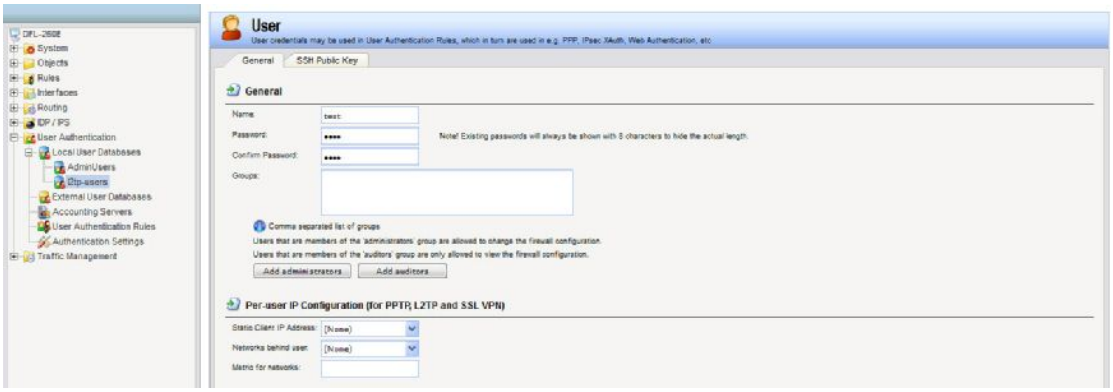
(7) Создаём новое IP правило для L2TP пользователей.



(8) Создаём базу данных для l2tp пользователей



(9) Добавляем в L2TP базу пользовательский аккаунт.



(10) Создаём правила аутентификации пользователей.