Создание Virtual Servers на DFL-800

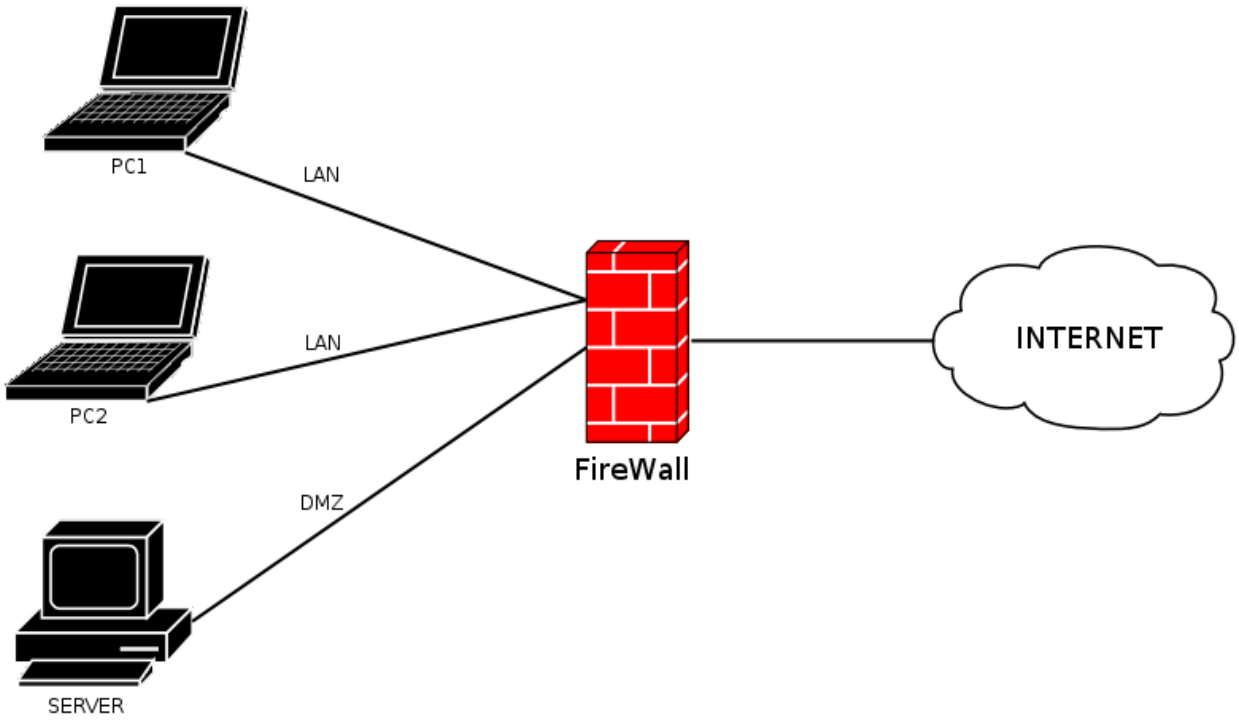
DMZ и Virtual Servers

DMZ – (Demilitarized Zone) - это дополнительная возможность межсетевых экранов серии DFL-XXX, предназначенная для предоставления доступа к внутренним (то-есть находящимися за firewall и защищенных NAT-ом) серверам (таким, как почтовый, WWW, FTP) пользователям из Интернет. В данном случае запрос извне на любой порт внешнего (WAN) интерфейса отображается на такой же порт компьютера, указанного в настройках DMZ.
То есть, все открытые порты на этом компьютере доступны снаружи. Это может создать угрозу безопасности для данного компьютера, в целях безопасности возможно использование Virtual Servers.
Virtual Servers – определяется фиксирование значение портов которые можно перенаправить к локальной сети через firewall. Переназначение портов защитит систему от возможных атак.

Рассмотрим настройку переназначения портов для DFL-800

Примичание: DFL-800 имеет объектный интерфейс, все действия ведутся с предопределёнными и созданными объектами.

Рассмотрим простейшую схему:



Нам нужно получить доступ по SSH к некоторой машине внутри сети через Интернет. По умолчанию, firewall не даст пройти сквозь защиту и обращение будет отброшено с соотвествующей записью в журнал событий(Log)

В логах это будет выражено вот так:

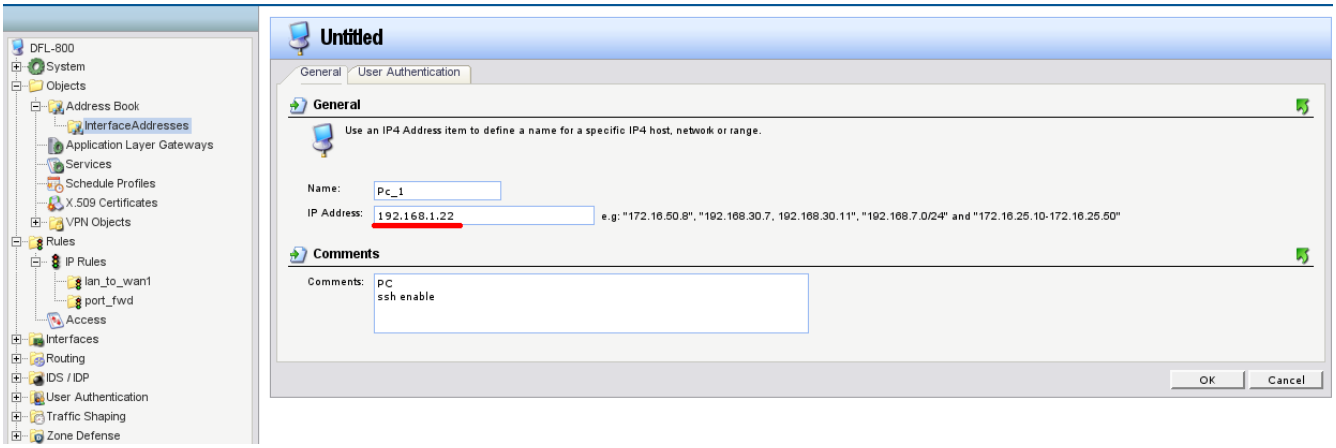
Date	Severity	Catergory	Rule	Proto	SrcIf	Src/DstIP	Src/DstPort	Details
2006-05-02 16:58:55	Notice	DROP	Default_Rule	TCP	wan1	192.168.100.1	192.168.100.239 55830 22	action=drop ipdatalen=40 tcphdrlen=40 syn=1
2006-05-02 16:58:52	Notice	DROP	Default_Rule	TCP	wan1	192.168.100.1	192.168.100.239 55830 22	action=drop ipdatalen=40 tcphdrlen=40 syn=1
2006-05-02 16:57:59	Notice	DROP	Default_Rule	TCP	wan1	192.168.100.1	192.168.100.239 55810 22	action=drop ipdatalen=40 tcphdrlen=40 syn=1
2006-05-02 16:57:56	Notice	DROP	Default_Rule	TCP	wan1	192.168.100.1	192.168.100.239 55810 22	action=drop ipdatalen=40 tcphdrlen=40 syn=1

Нужно создать и предопределить несколько объектов:

1. Создаём объект – IP адрес хоста к которому мы будем перенаправлять трафик

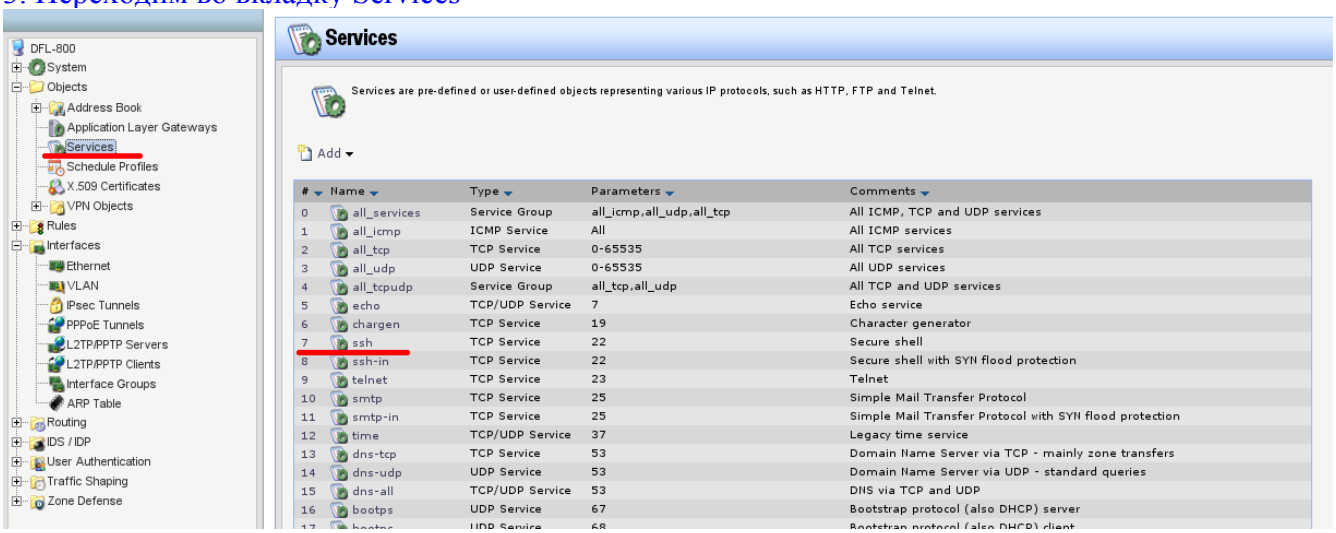
2. Выбираем пункт “IP4 host/network”

Добавляем IP адрес хоста к которому мы будем перенаправлять трафик

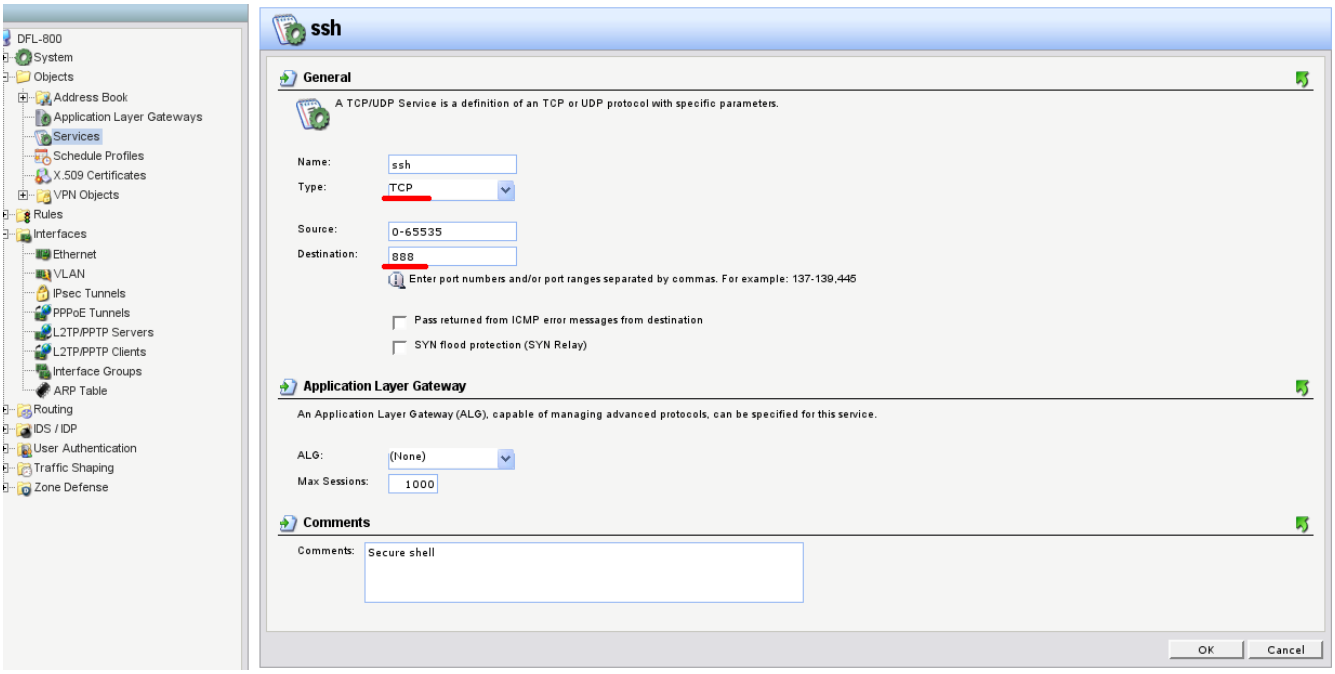


После добавления IP адреса внесём некоторые коррективы в созданный объект “Service”
Для примера будем использовать предопределенный объект для протокола SSH. Напомню, что наша задача получить доступ к управлению машиной по внешнему порту 888. Когда мы будем формировать обращение к серверу, то нужно указать порт не по-умолчанию, а порт 888.
Примичание: если Вы хотите не хотите изменять порты, то прорустите слудующие 2 шага
Изменим объект под использование другого порта

3. Переходим во вкладку Services



4. Выбираем проткол SSH

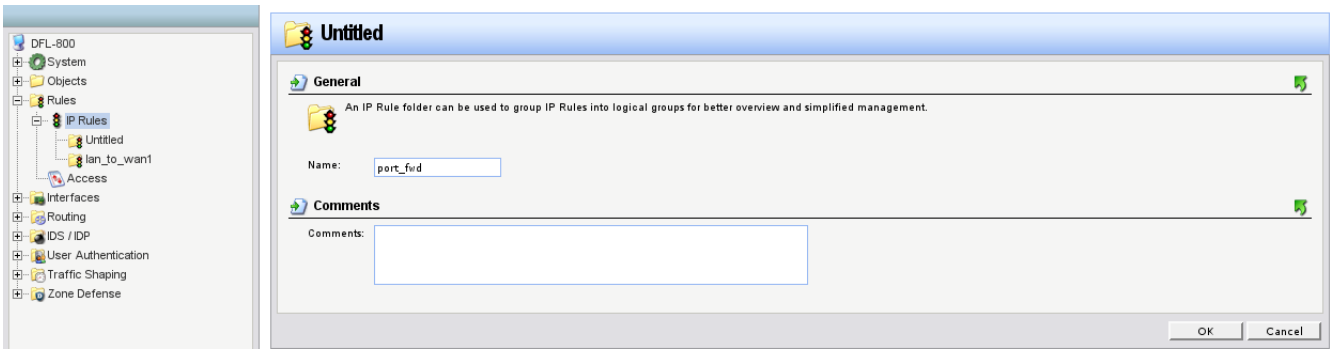


Изменям Destination порт. Source порт изменять не рекомендуется, клиентское приложение может использовать произвольный порт диапазона. Изменять можно, если заранее известен Source порт.

Когда протоколы предопределены, нужно настроить разрещающие правила для перенаправления портов и правило для firewall. В пришедшем пакете, сравниваются Src Port, Dest Port и Protocol. Если поля совпадут с предопределенным правилом, система будет искать следующее правило для пропуска пакета в зону lan.

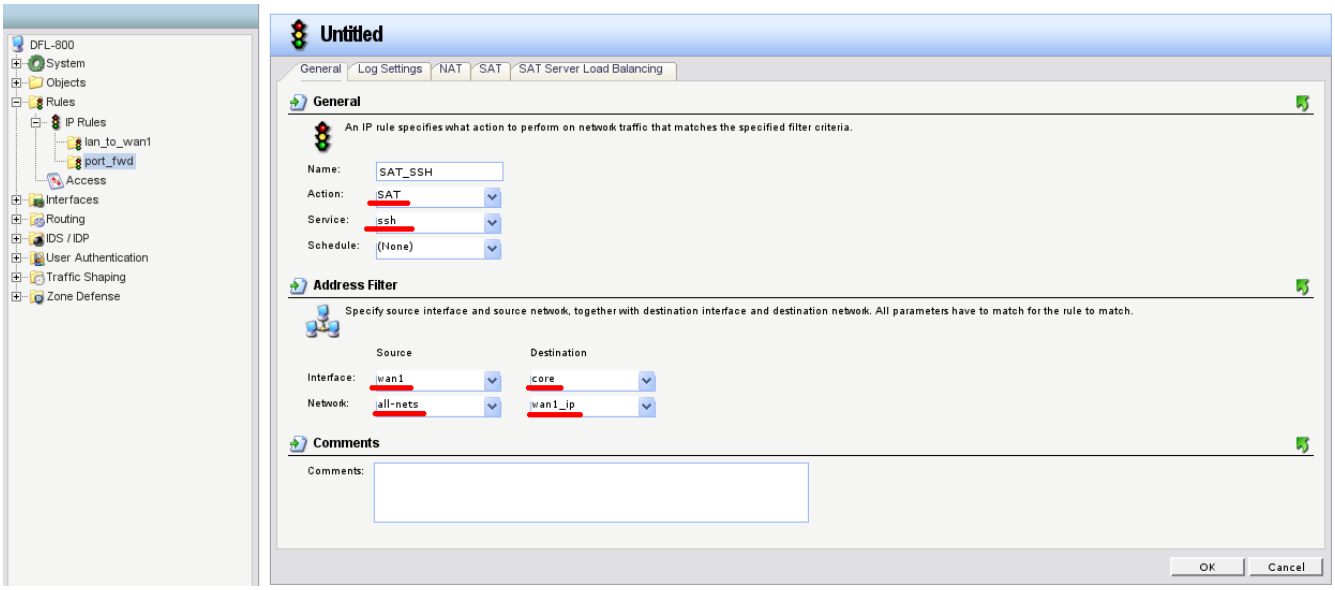
Создание правила для разрешения прохода в защищенную зону LAN

5. Создаём папку для предопределния правил для FW.

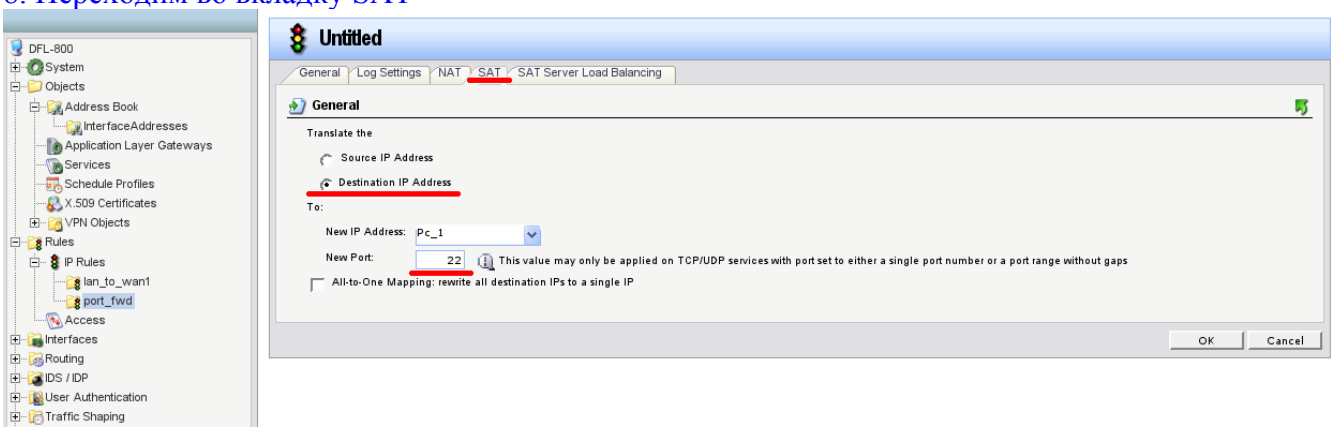


6. Выбираем вкладку IP Rule для создания нового правила

7. Создаём правило для перенаправления портов. Для этого предопределён параметр SAT(Static Address Translation)

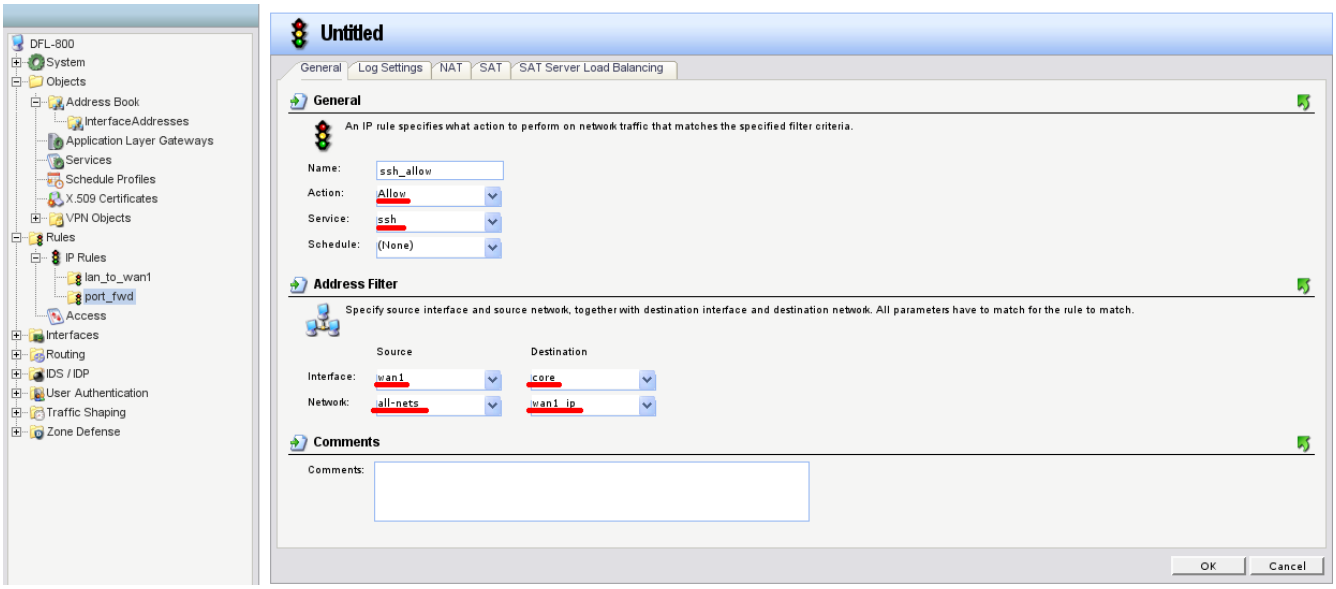


8. Переходим во вкладку SAT



9. Определяем на какой порт будут перенаправлятся данные.

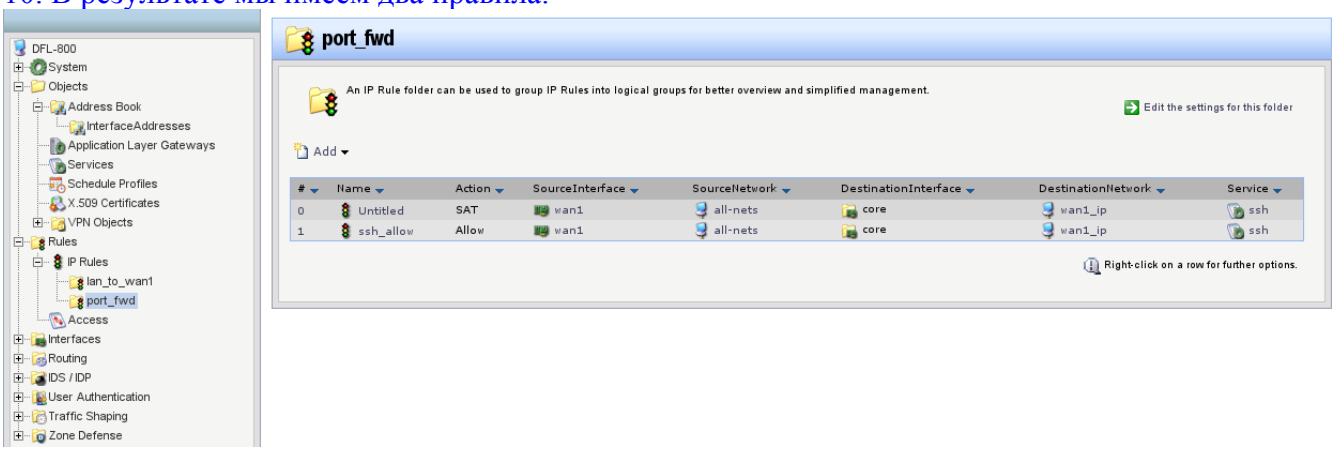
Примичание: Если Вы не предопределяли порт, то в поле "New Port" ничего вводить не нужно. Нажимаем OK и создаём новое правило для FW



В поле action выставить allow, что будет сообщать firewall, все пакеты совпавшие с правилом будут пропущены.

ЗАМЕЧАНИЕ:
При использовании перенапраления портов, в Destination Inerface необходимо указывать "Core"

10. В результате мы имеем два правила.



Примечание: За правилом SAT сразу же должно идти правило Allow, иначе firewall не пропустит пакет в зону LAN, к серверу.

Проверка работоспособности системы

Целью было перенаправить порт с внешнего интерфейса WAN во внутреннюю подсеть LAN. Для примера использовалося сервис SSH с 22 TCP портом для установления соединений. Предлагалось перенаправить с внешего порта 888 к внуреннему порту, через firewall, на порт 22 Для теста нужно подсоедениться к WAN порту с помощью кросс-патчкорда и запустить командную строку. Выполнение перенапраления портов можно проверить с помощью утилиты telnet.
Синтаксис: telnet <ip_host> <destination port>
В нашем случае команда будет выглядеть так:

```
MBS# telnet 192.168.100.25 888
Trying 192.168.100.25...
Connected to  Debi.msk.dlink.ru.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.2p1 Debian-7
```