

Удаленный доступ на объекты автоматизации

Инструкция по настройке маршрутизатора

Версия 1.0 [12.03.2015]

ООО “Симатек групп”, г.Минск

2015

Содержание

[ВВЕДЕНИЕ 3](#_Toc413943390)

[1 Настройка WAN интерфейса (интернет на маршрутизаторе) 4](#_Toc413943391)

[2 Настройка LAN-интерфейса (раздача интернета в локальную сеть) 9](#_Toc413943392)

[3 Настройка удаленного доступа на сервер в локальной сети объекта 15](#_Toc413943393)

[4 Настройка соединения VPN 19](#_Toc413943394)

[5 Обслуживание маршрутизатора 23](#_Toc413943395)

[6 Настройки режима Firewall в маршрутизаторе 24](#_Toc413943396)

# ВВЕДЕНИЕ

Инструкция посвящена настройке удаленного доступа на объекты автоматизации, на которых применяется типовое решение удаленного доступа компании «Симатек».

Маршрутизатор мы обычно поставляем нашему заказчику вместе с оборудованием для конкретного проекта.

От заказчика требуем обеспечить доступ в интернет. Можно с выделенным IP-адресом, **можно без** выделенного нам отдельного адреса, но тогда заказчик должен выполнить т.н. проброс портов со своего внешнего адреса на наш маршрутизатор. **Без выполнения одного из этих условий нет смысла читать данное руководство.**

Раздел 1 и 2 данного руководства посвящен настройкам маршрутизатора, которые позволяют организовать локальную подсеть (LAN), включить в нее сервера, АРМы и прочие устройства и раздать всем интернет-доступ из внешней сети (WAN).

В разделе 3 объясняется, как можно настроить доступ к конкретному серверу в локальной сети из любой точки интернета с использованием специальных программ удаленного доступа, таких, как Radmin и Remote Desktop Protocol.

Технология доступа с использованием VPN описывается в разделе 4. В нем объясняется, как можно настроить доступ из офиса компании в локальную подсеть объекта со всеми ее клиентами, серверами, контроллерами, панелями оператора и проч.

Раздел 5 посвящен общим настройкам маршрутизатора, например, сохранению удачной конфигурации и заданию нового пароля администратора.

Раздел 6 содержит базовые сведения о настройке режима Firewall.

Для полноценного доступа всеми перечисленными способами требуется выделенный статический адрес для маршрутизатора. В этом случае будет минимум настроек.

Если нет возможности получить статический IP, требуется следующий проброс портов:

-для VPN нужно пробросить порт 500 с внешнего статического адреса в сети интернет заказчика на внутренний адрес нашего маршрутизатора в его локальной сети на порт 500. Протокол UDP. Либо службу IKE.

-для Radmin и RDP нужен проброс любых портов. 501 и 502, к примеру, или более, в зависимости от количества серверов/АРМов, к которым нужен доступ.

# 1 Настройка WAN интерфейса (интернет на маршрутизаторе)

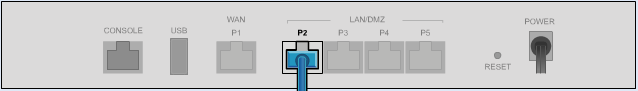
На момент написания руководства в типовом решении используется маршрутизатор Zywall серии USG.

WAN-порт – для внешнего подключения, интернет из сети заказчика по интерфейсу Etnernet либо интернет от локального ADSL модема с преобразованием в интерфейс Etnernet. Адресное пространство назначает заказчик статическим либо динамическим способом.

Интернет с выделенным/внешним IP-адресом (статический IP адрес) - очень хорошо. Маршрутизатор будет доступен из интернета, требуется произвести меньше всего настроек.

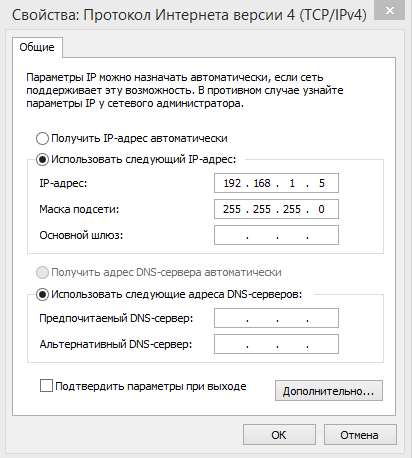
Интернет без выделенного/внешнего IP-адреса. От заказчика потребуется «проброс портов».

LAN-порты – для организации сети объекта, в которую могут входить АРМы, сервера, контроллеры. Адресное пространство произвольное, но выбранное согласно правилам построения IP сетей: 10.0.0.0—10.255.255.255; 172.16.0.0—172.31.255.255; 192.168.0.1—192.168.255.255.

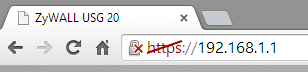


Первоначальная настройка: модем из коробки или после операции Reset имеет адрес 192.168.1.1 на порту LAN1. Доступ через веб-интерфейс по протоколу HTTPS. Адрес в браузере <https://192.168.1.1>, авторизация по умолчанию: admin/1234.

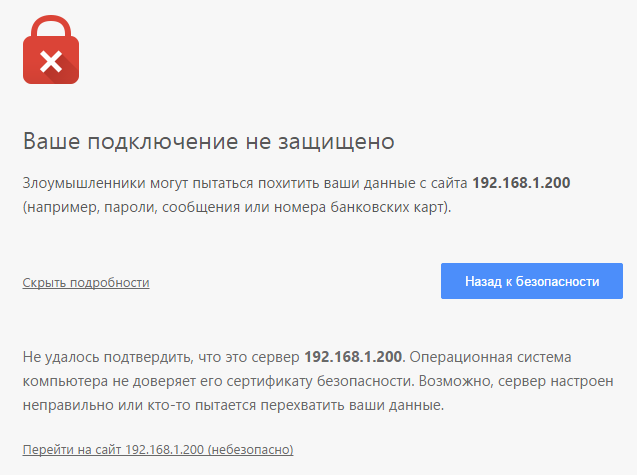
1. Соединяем маршрутизатор и ноутбук сетевым проводом в порт LAN1. Интернет от заказчика включаем в порт WAN.
2. Настраиваем свой сетевой адаптер, адресное пространство – статическое, адрес 192.168.1.5, как на рисунке:

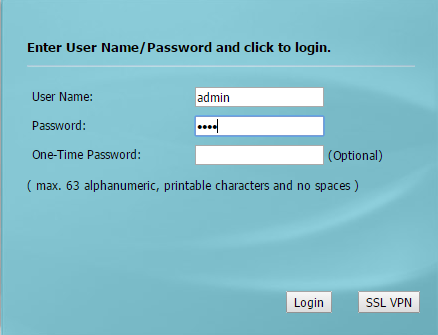


1. В браузере (лучше использовать IE) вводим адрес:

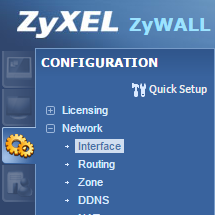


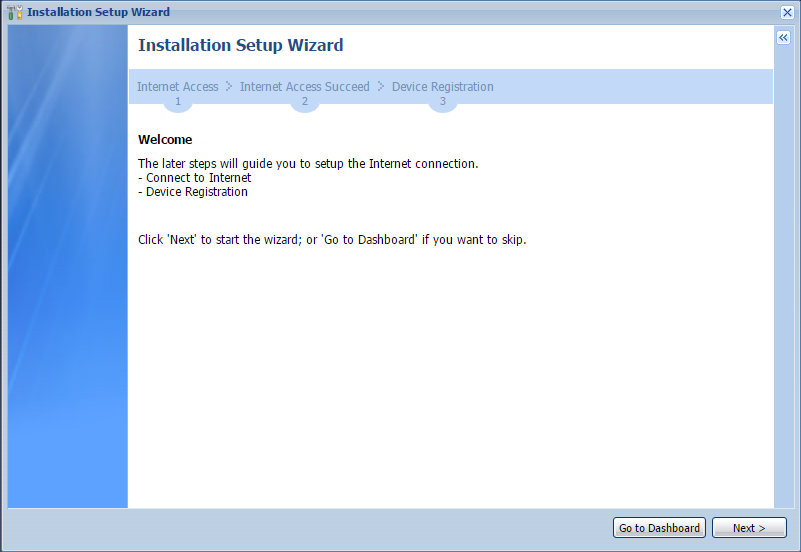
Если браузер ругается, как на рисунке, продолжаем настойчиво переходить по нужному адресу, пока не получим запрос на ввод логина-пароля. Логин **admin**, пароль **1234**. После настройки, само собой, рекомендуется изменить пароль.





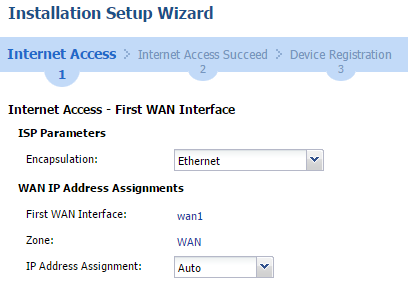
1. Настраиваем WAN-интерфейс. Мастер настройки запускается автоматически при первом входе. Вызвать его в любой другой момент можно по кнопке “Quick setup”:

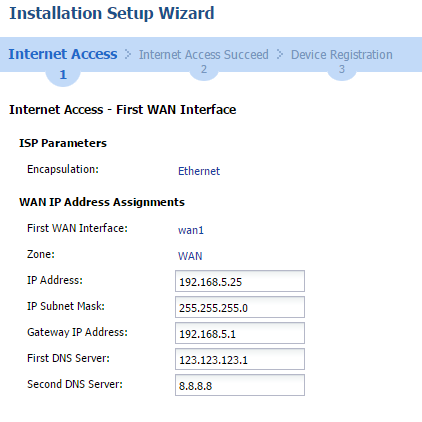




Настройка автоматическая, в стиле «Далее-Далее-Далее». Но есть 2 варианта:

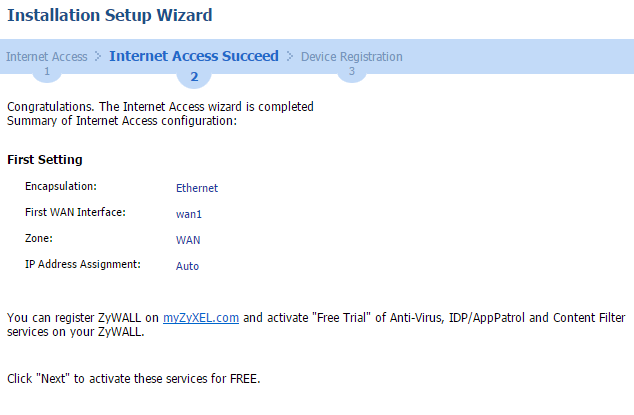
1. маршрутизатор получает IP адрес по порту WAN автоматически, так же как и адреса шлюзов, DNS, DHCP, WINS.
2. адреса настраиваются вручную, в этом случае поставщик интернета (заказчик) должен выдать, как минимум, адрес маршрутизатора, шлюза и DNS сервер.





После завершения работы мастера мы получаем интернет доступ на маршрутизаторе.

Далее необходимо раздать этот интернет всем устройствам в сети LAN.

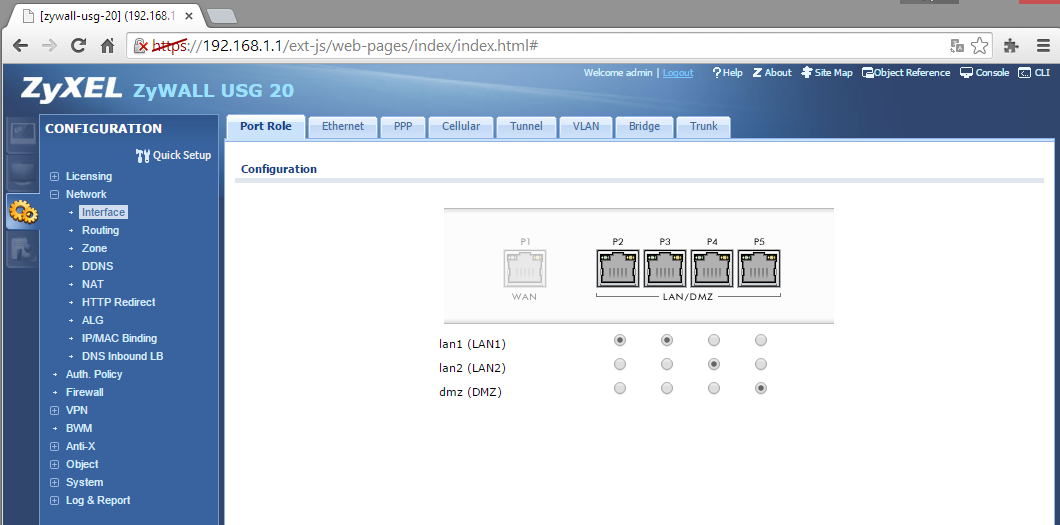


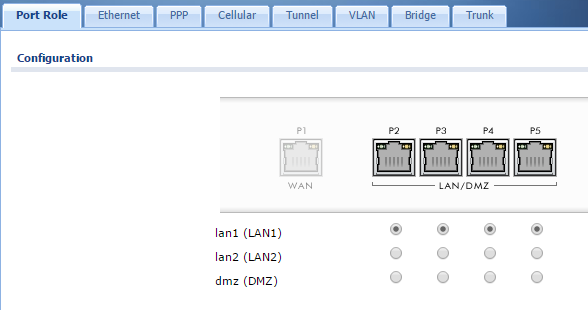
# 2 Настройка LAN-интерфейса (раздача интернета в локальную сеть)

В общих чертах: назначить порты LAN, определить адресное пространство, раздать маршрутизатором доступ всем клиентам, подключенным к сети LAN.

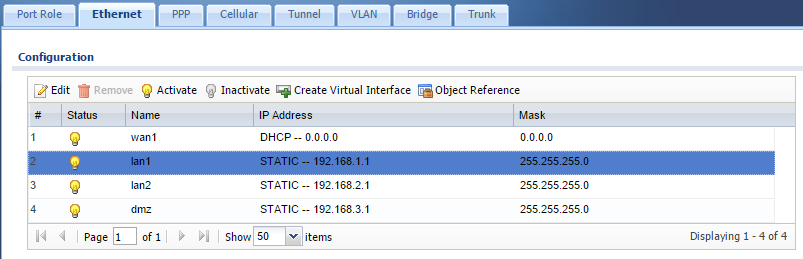
Роль портов настраиваем в разделе Configuration-Interface-Port Role.

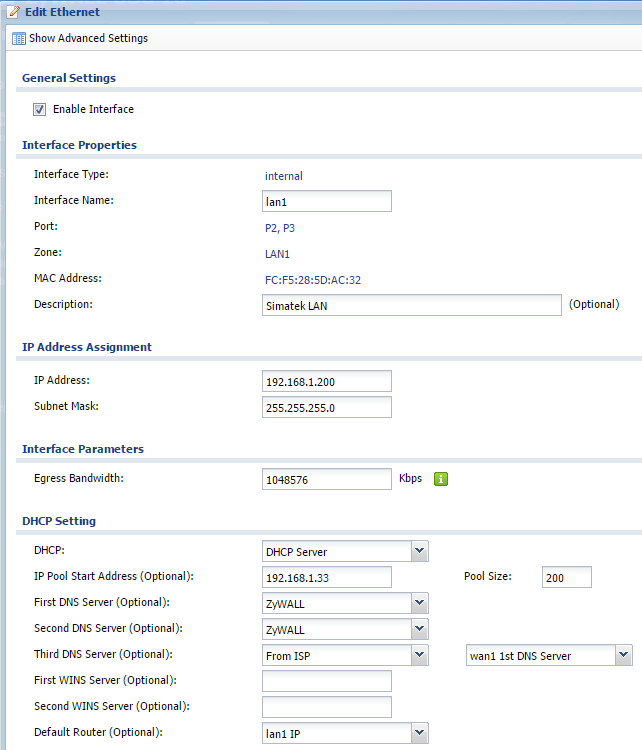
Если нет особых требований к использованию зоны DMZ, нескольких подсетей и т.д., то можно все порты маршрутизатора настроить как порты LAN1.





Далее открываем и редактируем свойства сети LAN1.





Выбираем адресное пространство. В данном примере **192.168.1.0**. Но оно может быть любым допустимым. Если нет особых требований, то лучше выбирать отличное от 192.168.0.0, т.к. это облегчает дальнейшую настройку удаленного доступа со стороны офиса, если планируется создавать VPN соединение.

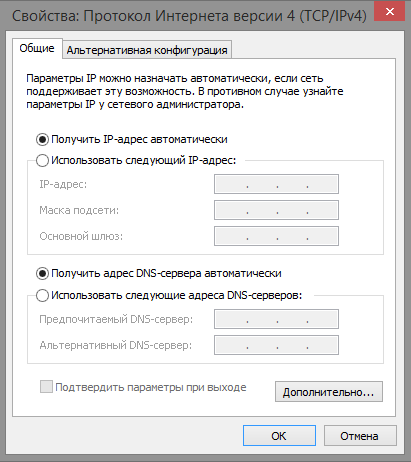
Например, можно выбрать третью цифру похожей на номер проекта: 192.**168**.**24**.0 (например, для проекта 7524). Но в целом вопрос не критичный и остается на усмотрение специалиста, читающего данное руководство.

Итак, выбрали подсеть LAN 192.168.1.0, маршрутизатору назначили адрес 192.168.1.200.

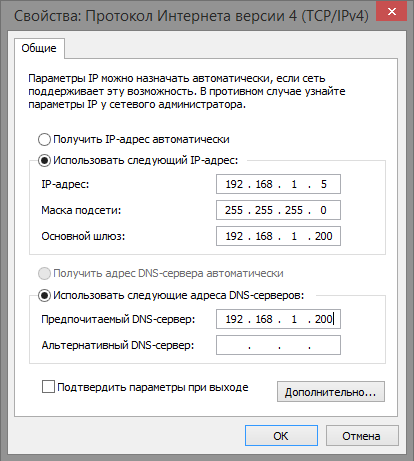


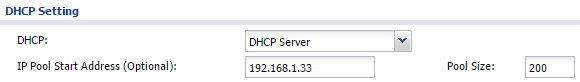
Далее необходимо определить роль маршрутизатора.

1. DHCP –сервер. Маршрутизатор автоматически раздает всем клиентам, подключенным в сеть LAN, IP-адрес, адрес шлюза и DNS сервера, интернет. В этом случае в свойствах сетевого адаптера каждого подключенного клиента не нужно ничего настраивать.



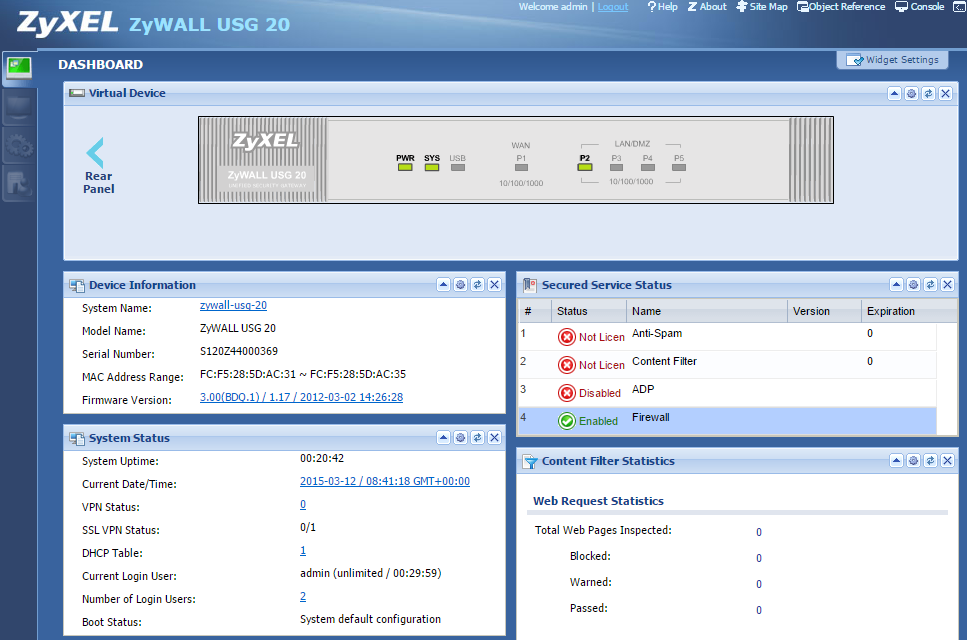
1. DHCP сервер выключен. На каждом подключенном клиенте необходимо будет назначить адрес, маску, шлюз, DNS-сервер. Шлюз – адрес самого маршрутизатора. Шлюз используется для доступа в интернет.

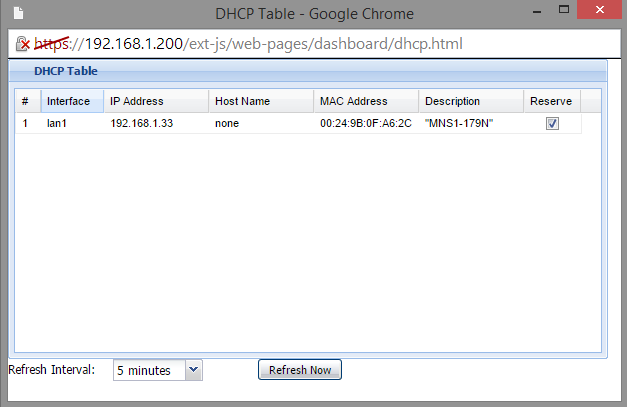




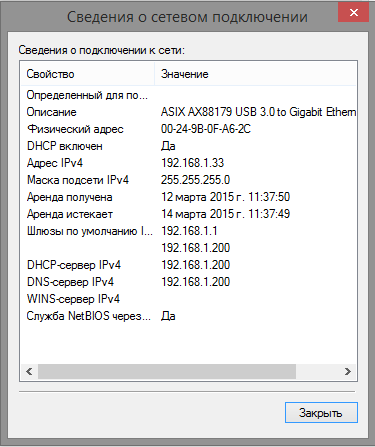
Режим DHCP-сервера удобней. Все раздается автоматически. Адреса выдаются из пула, стартовый адрес и размер пула настраиваются. Если необходимо, чтобы какое-то устройство в сети имело неизменный адрес, можно настроить конкретно это устройство вручную либо выполнить операцию привязки IP-адреса к MAC-адресу устройства, тогда DHCP-сервер будет назначать этому устройству всегда один и тот же адрес. По-крайней мере, пока не заменят сетевой адаптер в данном устройстве.

Привязка выполняется через DHCP-таблицу, доступ к которой есть на странице Dashboard, как показано на следующих двух рисунках.

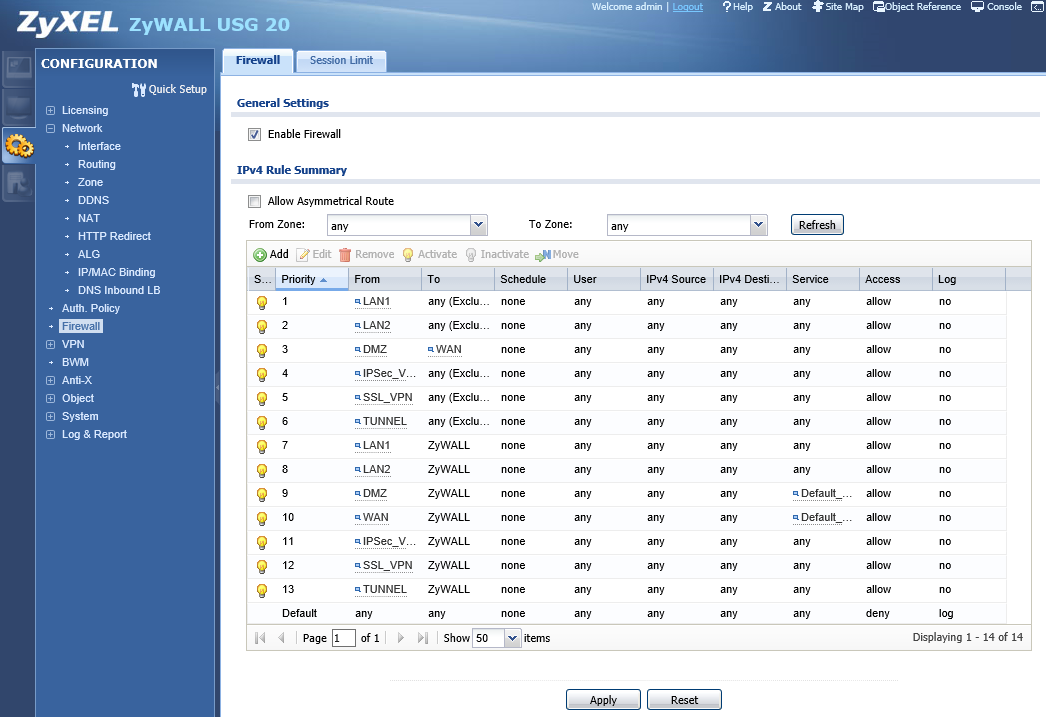




После настройки WAN и LAN все ваши клиенты должны иметь доступ к сети и к интернету:



Если имеются проблемы с доступом, для начала отключите в маршрутизаторе режим Firewall:



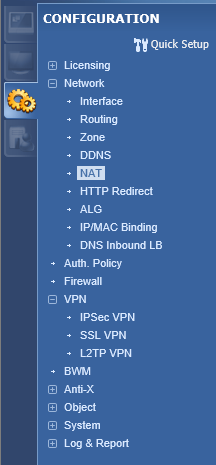
# 3 Настройка удаленного доступа на сервер в локальной сети объекта

Исходные условия: настроена раздача доступа в интернет в сети LAN через маршрутизатор. Имеется IP-адрес маршрутизатора в сети Internet либо настроен проброс через оборудование поставщика интернета. Цель – получить доступ на сервер в сети объекта через программы Radmin и RDP.

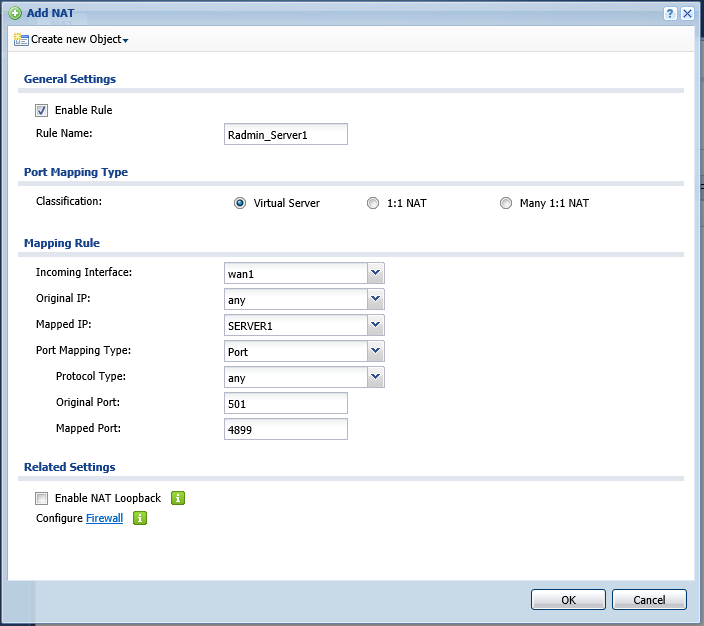
Для настройки используется технология NAT. В двух словах это когда один IP-адрес, например 88.89.90.15 позволяет получить доступ к нескольким компьютерам с помощью использования проброса портов, т.е. дописывая номер порта в конце адреса 88.89.90.15:501, 88.89.90.15:502 мы получаем возможность переадресовывать наши запросы извне на любые адреса в нашей внутренней сети.

Как это работает. Есть статический IP в сети интернет, например, 88.89.90.15. Он назначается как WAN-адрес нашего маршрутизатора. По нему мы можем получить доступ на сам маршрутизатор. Далее настраиваем проброс с маршрутизатора на сервер в нашей локальной сети, например, адрес 88.89.90.15:502 -> отправит нас на внутренний адрес сервера 192.168.1.33:3389.

Настройка NAT. Заходим в раздел Configuration – Network - NAT



Нажимаем кнопку Add (добавить правило).

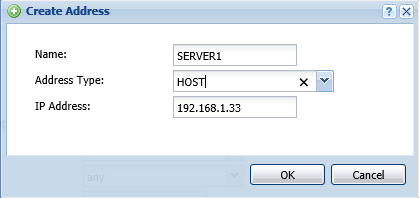


Создаем правило для программы Radmin.

Incoming interface: WAN1 (входящий извне)

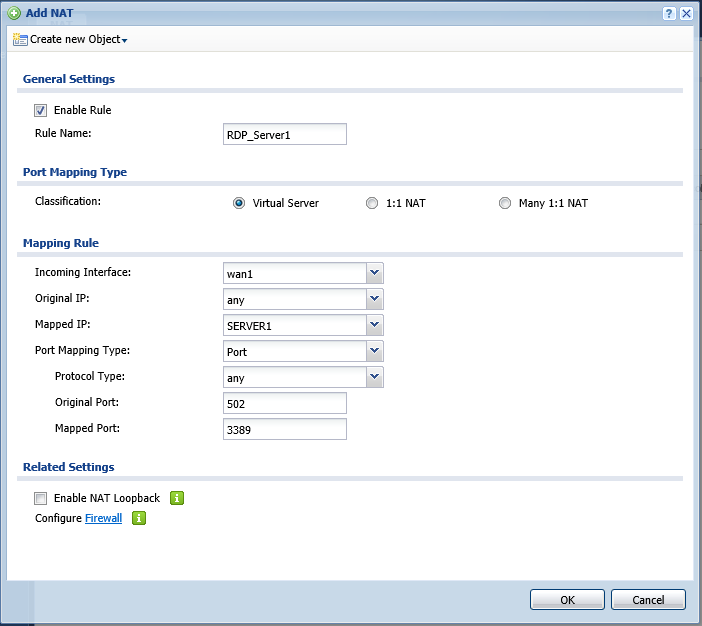
Original IP: any (входить можно с любого адреса интернет)

Mapped IP: 192.168.1.33 или SERVER1 (имя к адресу можно привязать, нажав кнопку Create New Adress)

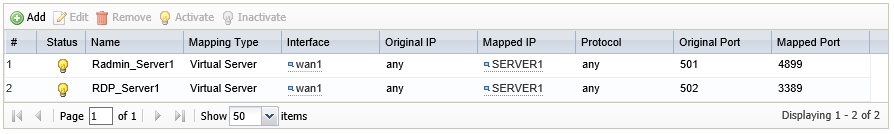


Далее указывается, с какого входящего порта (произвольный) нужно транслировать запрос на конкретный порт сервера во внутренней сети. Если используется программа Radmin с настройками по умолчанию, то необходимо указать конечным портом 4899.

Аналогичным образом настраивается проброс порта для любой другой программы. Например, настройки для стандартного RDP (Remote Desktop Protocol – Удаленный рабочий стол) выглядят следующим образом.

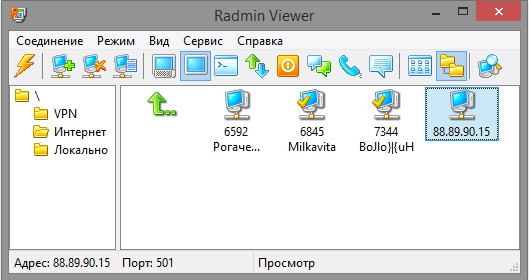


После создания правил можем наблюдать их активный статус в разделе NAT.



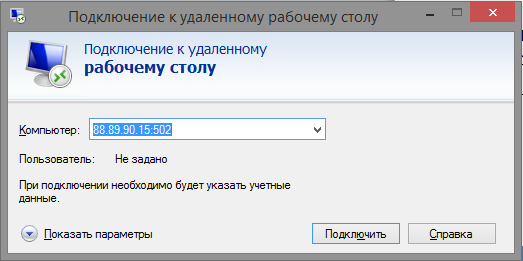
Не забываем, если включен режим Firewall, необходимо внести изменения в его настройки, чтобы правильно заработал NAT. Важно! NAT срабатывает перед firewall, т.е. настраивать безопасность нужно уже для транслированных адресов.

После настройки трансляции адресов получаем доступ через интернет к нашему серверу, например, через Radmin:



Подключение на адрес из нашего примера 88.89.90.15:501 транслируется на адрес 192.168.1.33:4899, т.е. на сервер в локальной сети объекта на порт программы Radmin.

То же самое справедливо для Удаленного рабочего стола:



Подключение на адрес из нашего примера 88.89.90.15:502 транслируется на адрес 192.168.1.33:3389, т.е. на сервер в локальной сети объекта на порт программы RDP.

Не только в данном примере, но и в реальности, порт 4899 является стандартным портом программы Radmin, а порт 3389 стандартным портом программы RDP.

Технология NAT позволяет организовать удаленный доступ и **без фактической привязки выделенного статического адреса к нашему маршрутизатору**. Если у заказчика есть свой (например, заводской) выделенный IP, они могут сделать проброс портов на наш маршрутизатор.

# 4 Настройка соединения VPN

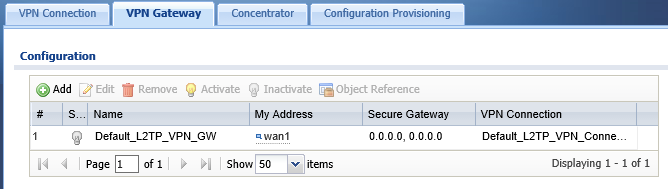
В общих чертах: VPN – Virtual Private Network. Доступ не на отдельно взятый компьютер, а к целой подсети. Можно организовать доступ из сети офиса в подсеть конкретного объекта автоматизации со всеми подключенными к ней панелями оператора, контроллерами, серверами и АРМами. Доступ к подсети означает полноценную работу любых сетевых программ, помимо radmin и RDP можно использовать файловые менеджеры или спецсофт (например, наблюдать режим онлайн в контроллере или заливать проект в панель оператора).

При этом VPN-канал, после первоначальной настройки, подключается автоматически, благодаря тому, что в офисе установлен и работает VPN-сервер.

Для настройки VPN необходимо знать IP-адрес маршрутизатора в офисе и на объекте (еще раз напоминаю, что на объекте он может быть не отдельно выделенным, а транслированным через технологию проброса портов).

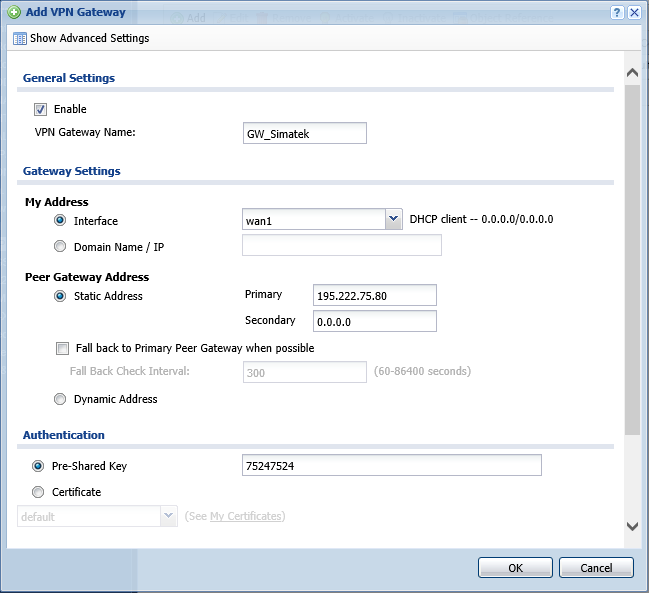
Итак, настройки выполняются в разделе **Configuration – VPN – IPSec VPN**

Сначала создается шлюз (VPN Gateway) , а затем соединение (VPN Connection) через этот шлюз.



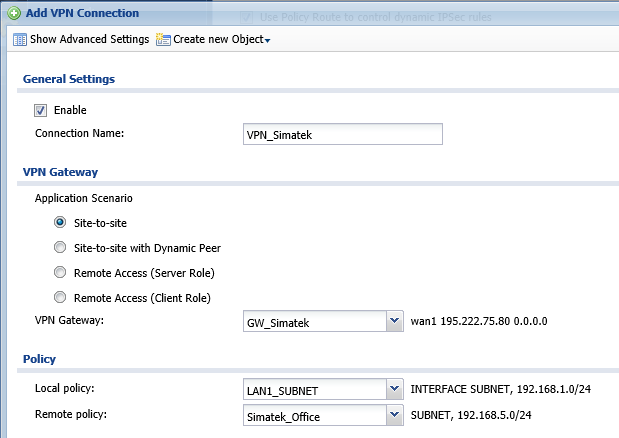
В настройках шлюза необходимо указать адрес маршрутизатора в офисе и ключ сети.

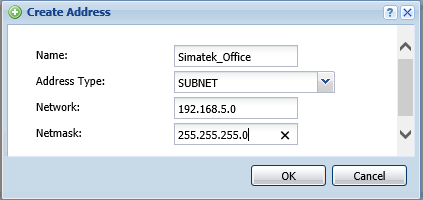
Адрес офиса Simatek 195.222.75.80. Ключ назначается любой, главное, чтобы он был одинаковый на объекте и на стороне офиса ☺



После того, как шлюз создан, необходимо создать соединение VPN.

В настройках соединения выбирается только что созданный нами шлюз, тип Site-to-site, а также политика для локальной и удаленной сети. Локальная сеть это LAN1. В нашем примере она имеет адресное пространство 192.168.1.0. В списке объектов она присутствует под именем LAN1\_SUBNET, причем присутствует изначально, по-умолчанию. А вот подсеть, которая со стороны объекта будет считаться удаленной (т.е. подсеть офиса) нужно создать в списке объектов, перед тем, как выбрать. Нажимаем кнопку Create New Object и создаем новый объект типа SUBNET с адресным пространством **192.168.5.0.**

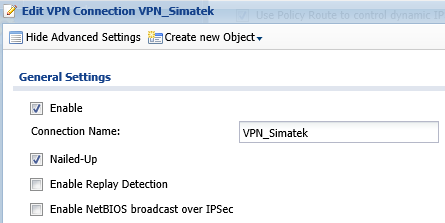




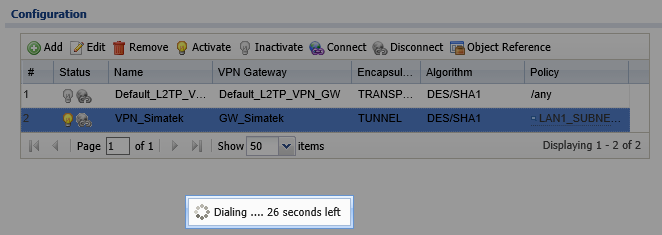
Со стороны офиса на офисном маршрутизаторе выполняются аналогичные настройки. После этого можно работать в подсети объекта, находясь в офисе! Ура.

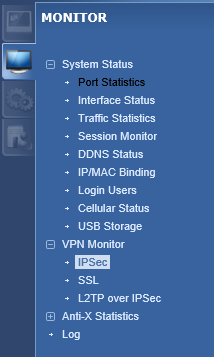
Если соединение не устанавливается, необходимо убедится в наличии интернет доступа и проверить настройки Firewall на маршрутизаторе на объекте и в офисе.

Если необходимо, чтобы VPN-соединение устанавливалось автоматически, можно включить опцию Nailed-Up:



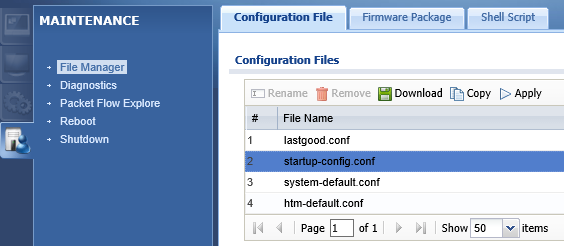
Если все прошло успешно, можно наблюдать значок подключенного VPN –соединения в списке соединений и в разделе Monitor-VPN Monitor-IPSec, а также в логах.



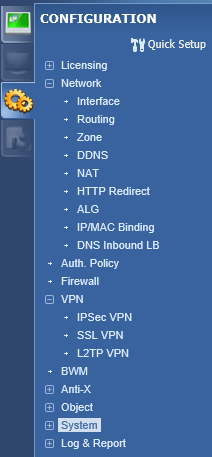


# 5 Обслуживание маршрутизатора

Сохранить успешную конфигурацию можно в разделе Maintenance-File Manger



Задать новый администраторский пароль на доступ к маршрутизатору можно в разделе Configuration – System – Object – User/Group



# 6 Настройки режима Firewall в маршрутизаторе

Если вы не знаете, что такое firewall и не представляете, как его настраивать, лучше отключите этот режим в маршрутизаторе.

