УДАЛЕННЫЙ ДОСТУП К КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ VPN

Ярмак Д.А. Email: Yarmak1134@scientifictext.ru

Ярмак Дмитрий Анатольевич - студент магистратуры,
физико-технический факультет,
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
Кубанский государственный университет, г. Краснодар

Аннотация: *в статье рассматривается пример удаленного доступа на сеть предприятия. Есть 4 основных типа реализации такой системы, рассматривать все мы не будем, рассмотрим только одну. Данной системы у нас в университете нет, поэтому хотел реализовать данный пример для дальнейшего обучения студентов. В данной статье будет использовано оборудование производства Cisco, так как это самая доступное и часто используемое оборудование. Также будут использованы сервера и пример конфигурации для работоспособности данной схемы. Какие - мы рассмотрим далее.*
Ключевые слова: *VPN, сервер с TMG, активном каталоге, сервер терминалов.*

REMOTE ACCESS TO THE CORPORATE NETWORK VIA VPN

Yarmak D.A.

Yarmak Dmitriy Anatolevich – graduate student,
PHYSICAL-TECHNICAL FACULTY,
FEDERAL STATE BUDGETARY EDUCATIONAL INSTITUTION OF HIGHER PROFESSIONAL EDUCATION KUBAN STATE UNIVERSITY,
KRASNODAR

Abstract: *the article is an example of remote access to the enterprise network. There are 4 main types of implementation of such a system, we will not consider all of them, we will consider only one. We do not have this system at our university, so I wanted to implement this example, for further training of students. In this article, Cisco equipment will be used, as this is the most affordable and frequently used equipment. In the same way, the server and the configuration example for the operation of this circuit will be used. Which we consider below.*
Keywords: *VPN, Server, TMG, Active directory, terminal Server.*

УДК: 654.9

Начнем с того, что собственно такое VPN - это технология, обеспечивающая защищённую (закрытую от внешнего доступа) связь логической сети поверх частной или публичной при наличии высокоскоростного интернета [2].

Я хочу рассказать об одном из решений, которое действительно работает, на собственном опыте. Отличие описано в 3 пунктах:

1. На стороне пользователя необходимо минимальное вмешательство в настройки — необходим стандартный функционал ОС Windows;
2. Удаленный пользователь работает на сервере терминалов, что обеспечивает его необходимой средой для выполнения своих должностных обязанностей
3. Легкое управление доступом к ресурсам предприятия

Начнем с того, что нам необходимо:

Сервер с TMG и Сервер терминалов На предприятии эти два сервера — виртуальная машина, подключенная на hyper-v.

Еще нам необходимы 2 не занятые сети. Предоставление доступа к ресурсам разделим на три этапа:

1. Доступ pptp в изолированную сеть vpn-клиентов
2. Доступ по rdp на сервер терминалов
3. Прямой доступ с сервера терминалов к ресурсам компании по любой маске

4. Доступ с помощью pptp в сеть vpn-клиентов

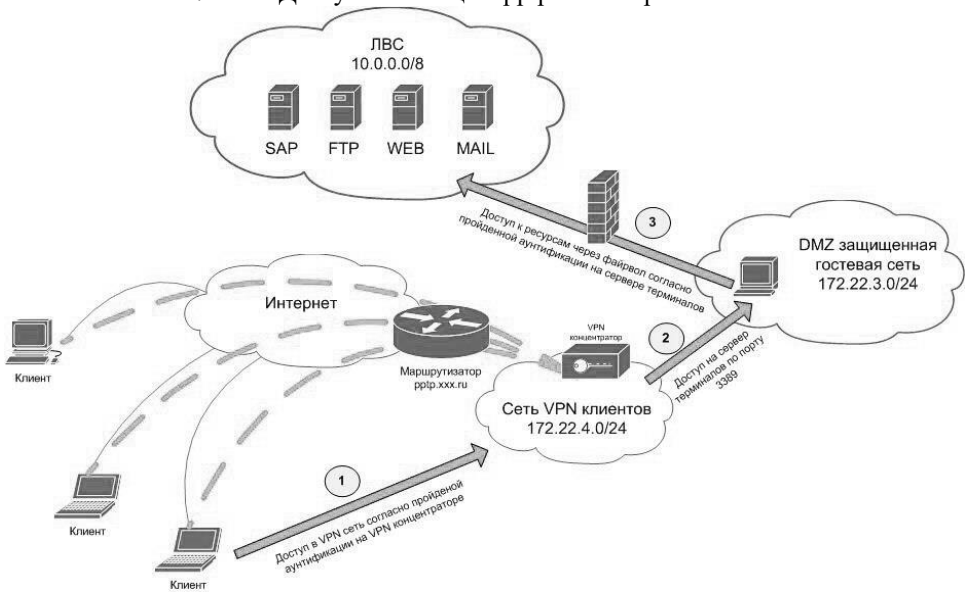

Рис. 1. Общая схема подключения и описание этапов

Доступ с помощью pptp в сеть vpn-клиентов. Для того чтобы воплотить это, необходим pptp сервер, будем пользоваться cisco, ничего не мешает прописать pptp с пограничного маршрутизатора\ firewall на TMG\ISA, которой будем пользоваться для доступа клиентов к ресурсам и поднять pptp сервер на ней. Ниже представлена часть конфигурации, которая отвечает за pptp.

```
vpdn enable
!
vpdn-group 1
! Default PPTP VPDN group
accept-dialin
protocol pptp
virtual-template 1
ip pmtu
ip mtu adjust

username ras_user password 7 0101570109065500755818OC4F044011530F5D2F7A743B62643
14255
username ras_guest password 7 120B541640185F3B7E2C713D653075005F025A

interface GigabitEthernet0/0.3
description Internet
encapsulation dot1Q 3
```

```
  ip address x.x.x.x 255.255.255.252
  ip nat outside
  ip virtual-reassembly max-fragments 64 max-reassemblies 256
  ip policy route-map Internet-10-144-68
  no cdp enable

  interface Virtual-Template1
  mtu 1400
  ip unnumbered GigabitEthernet0/0.3
  ip access-group 170 in
  ip tcp adjust-mss 1360
  peer default ip address pool vpn_users
  no keepalive
  ppp encrypt mppe auto
ppp authentication ms-chap-v2
ppp ipcp dns 172.22.1.201
!
ip local pool vpn_users 172.22.4.1 172.22.4.250

access-list 170 permit udp 172.22.4.0 0.0.0.255 host 172.22.1.201 eq domain
access-list 170 permit tcp 172.22.4.0 0.0.0.255 host 172.22.3.1 eq 3389
access-list 170 permit icmp any any
access-list 170 permit tcp 172.22.4.0 0.0.0.255 host 172.22.3.1 eq www
```

Важнейший момент — организация сети vpn-клиентов с возможностью соединения из нее только на сервер терминалов на порт rdp.

Доступ по rdp на сервер терминалов.

Клиент подключен к pptp [3] серверу и имеет доступ на сервер терминалов, благодаря удаленному рабочему столу реализуется подключение к серверу терминалов, учетные данные при подключении — доменная учетная запись пользователя. Тут необходимо немного пояснить: В активном каталоге создаются группы согласно маске, предположим у нас четыре группы ресурсов, поделенные по темам. Тема 1, Тема 2, Тема 3 и общие. Следовательно в активном каталоге делаем 4 группы безопасности, так же сделаем Тема 1, Тема 2, Тема 3 участниками группы «общие». А группе «общие» сделаем доступ на сервер терминалов. Для подключения удаленного доступа каждому пользователю AD мы будем добавлять его в нужную группу.

Прямой доступ с сервера терминалов к ресурсам компании по любой маске доступа.

Для воплощения этого в жизнь потребуется настроить TMG\ISA, так как данная статья не носит в себе смысла инструкции, не будем детально рассматривать настройки firewall, выделим важные моменты:

- В TMG внешней сетью является наша локальная сеть [1].
- Внутренней является сеть с сервером терминалов.
- На сервере терминалов находится TMG\ISA клиент (других вариантов нет), это необходимо, чтобы мы могли присваивать нужные правила пользователям.
- Следовательно все правила в firewall присваиваются к созданным нами группам Тема 1, Тема 2, Тема 3 и общие.

Список литературы / References

1. *Мельников Д.А.* Системы и сети передачи данных: учебник. А. Мельников. М., 2013.
2. *Олейник А.И., Сизов А.В*. ИТ-Инфраструктура, 2001 г.
3. *Кочукова Е.В., Павлова О.В., Рафтопуло Ю.Б.* Система экспертных оценок в информационном обеспечении учёных // Информационное обеспечение науки. Новые технологии: Сб. науч. тр. М.: Научный Мир, 2009. С. 190-199.