

Техническое задание на проектирование сети ООО “Организация”

Общие положения

Техническое решение по проектированию сети ООО Организация должно состоять из двух основных частей:

- Предлагаемая аппаратная часть
- Программная часть – описание настроек и конфигураций аппаратной части.

Для подготовки ТЗ компанией Организация подготовлено:

- Схема сети
- Доступное на текущий момент для реализации оборудование (в наличии в компании Организация)
- Техническое задание

Основные требования к реализации сети ООО “Организация”:

1. Должна быть реализована на оборудовании одного производителя, количество используемых моделей оборудования должно быть сведено к минимуму (взаимозаменяемость оборудования)
2. Правила, определяющие, как работает сеть (листы доступа, исключения и т.д.) должны быть прописаны по URL – адресам, а не по IP адресам.
3. Сетевое оборудование (маршрутизаторы, файрволы) должны обеспечивать работу минимум с двумя провайдерами, обеспечивая автоматическое переключение с одного на другой в случае отказа в предоставлении услуг.
4. Должна быть возможность построения VPN каналов между офисами компании Организация со 128 битным шифрованием (IPSEC). Каналы должны строиться между всеми возможными провайдерами с обеих сторон с возможностью автоматического переключения каналов в случае автоматического переключения провайдеров на сетевом оборудовании.
5. Удаленное подключение к сети ООО Организация для удаленно работающих сотрудников должно выполняться при помощи VPN – клиента, проверка прав доступа должна выполняться при помощи Active Directory
6. Работа сотрудников компании в интернете должна осуществляться через Proxy (или существующее решение – Squid + WRSpy или альтернативное решение, предполагающее наличие черных и белых (нетарифицируемых) списков сайтов, контроль объема полученной информации, блокировку пользователей при превышении лимита полученной информации, а также возможность сохранения и просмотра логов посещения интернет).
7. Для решения должна быть предусмотрена возможность масштабирования (с учетом количества возможных VPN соединений).
8. Должна быть предусмотрена возможность сбора логов с сетевых устройств и сохранения их на сервере.
9. По итогам настройки сети должна быть составлена инструкция по выполнению типовых операций на сетевом оборудовании.

Требования к конфигурации сети

1. Общие для всех сайтов (центральный офис + регионы):
 - 1.1. Доступ извне к ресурсам сети закрыт, за исключением специально оговоренных случаев (WEB сайт для работы торговых агентов 192.168.10.234:8088)
 - 1.2. Доступ изнутри сети к ресурсам интернет закрыт, за исключением:

- 1.2.1. Для серверов (не терминальных) – открыто все.
- 1.2.2. Для терминальных серверов – открыто все, кроме доступа к WEB сайтам по протоколам http и https
- 1.2.3. Для рабочих станций закрыто все, кроме:
 - 1.2.3.1. Доступ помимо Proxu
 - 1.2.3.1.1. Доступ к Office365
 - 1.2.3.1.2. Доступ к Lync
 - 1.2.3.1.3. Доступ к Skype
 - 1.2.3.2. Доступ через Proxu
 - 1.2.3.2.1. http
 - 1.2.3.2.2. https
- 1.2.4. Для отдельных рабочих станций открыть доступ (центральный офис)
 - 1.2.4.1. Пенсионный фонд
 - 1.2.4.2. Налоговая инспекция
 - 1.2.4.3. Таможенное ПО
- 1.3. Для WIFI точек доступа:
 - 1.3.1. Для внутренних (ОрганизацияInt)
 - 1.3.1.1. открыт полный доступ во внутреннюю сеть.
 - 1.3.1.2. Доступ к внешним ресурсам осуществляется так же, как в пункте 1.2.
 - 1.3.2. Для внешних (ОрганизацияGuest)
 - 1.3.2.1. Доступ к внутренним ресурсам закрыт полностью
 - 1.3.2.2. Доступ к внешним ресурсам неограничен
 - 1.3.2.3. Рассмотреть возможность ограничения доступа сотрудников компании к гостевому WIFI (в том числе с собственных устройств)
- 1.4. Доступ к 10 подсети (материнская компания Rexel)
 - 1.4.1. Осуществляется только через центральный офис
 - 1.4.2. Доступ извне закрыт, кроме:
 - 1.4.2.1. ПО обмена данными с AD материнской компании
 - 1.4.2.2. ПО синхронизации паролей в AD (с материнской компанией)
 - 1.4.3. Доступ изнутри открыт полностью.
- 2. Регионы:
 - 2.1. Выход в интернет локально (не через центральный офис)
 - 2.2. Получение обновлений ПО (WSUS, Symantec antivirus) локально только на сервера
 - 2.3. Выход в 10 подсеть (материнская компания Rexel) через центральный офис (через VPN с центральным офисом)
- 3. Центральный офис
 - 3.1. Выход в 10 подсеть (материнская компания), в том числе регионы
 - 3.2. Удаленный доступ для сотрудников
 - 3.3. Терминал работы со Сбербанком

