

# 1. Техническое задание

Приветствую

У меня задача такая обеспечить работу бухгалтерской сети с защитой информации от внешних угроз, что бы была резервная линия постоянного выхода в интернет, цена готового решения должна быть до 2500\$.

Партнер прорабатывает вот какое решение, в принципе готов все сделать на Cisco, помогите с решением.

1 Вариант(Cisco):

Коммутатор: Cisco WS-C2960-24TT-L Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image

Маршрутизатор: Cisco 1811/K9 Dual Ethernet Security Router with V.92 Modem Backup

Межсетевой экран: Cisco ASA5505-50-BUN-K9 ASA 5505 Appliance with SW, 50 Users, 8 ports, 3DES/AES

Насколько в этом варианте нужен межсетевой экран поскольку в маршрутизаторе вроде бы есть какой то встроенный фаерволл.

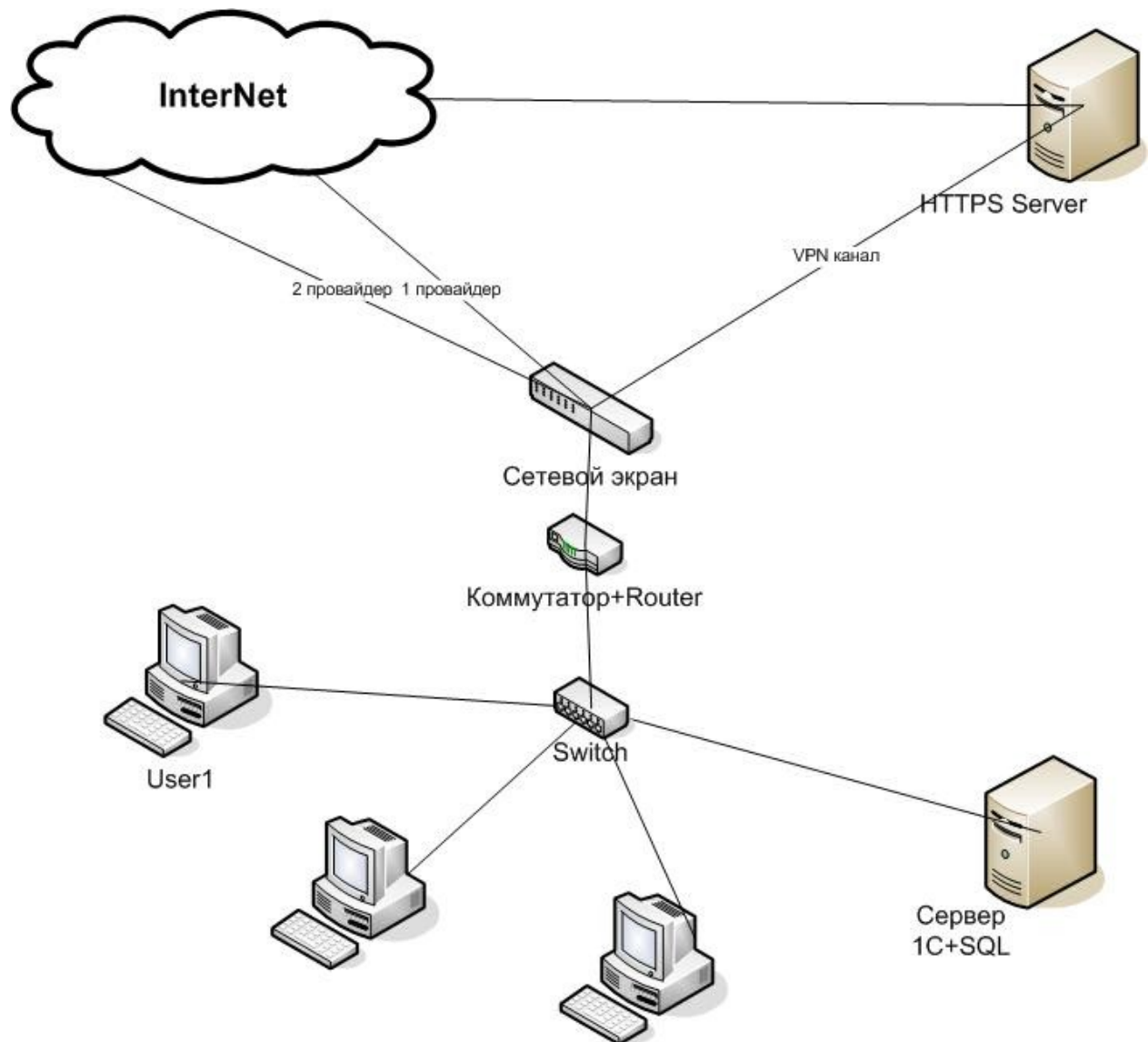
2 Вариант(D-link):

Коммутатор: D-Link Des-3526 или Des-1226G

Межсетевой экран D-Link DFL-1500 (Встроенный маршрутизатор)

Если кто то пользовался DLF-1500 как выполнен симбиоз 2 устройств нет ли конфликтов, насколько удобно управление, стоит ли покупать отдельные устройства или лучше использовать такой вариант.

Т.к я первый раз встречаюсь с таким оборудованием то хотел бы услышать ваши рекомендации тех кто работал с подобным оборудованием или обеспечивал работоспособной подобных сетей.



Защита обеспечивается для:

Базу sql 1с, трафик через https, доступ к машинам локальной сети. Вот то что нужно защитить. Потому как высока вероятность что будут попытки взломать сервер(получить доступ к базам к документообороту) либо вывести его из строя. Планируется сильно ограничить доступ в интернет с целью уменьшить вероятность получения троянов. Доступ будет только к определённым доменам. А вот с оборудованием ни как определиться не можем. Нужен нам сетевой экран, маршрутизатор как отдельные устройства или можно взять сплит систему.

- К Серверу SERVER 1C+SQL хотелось что бы вообще доступа с интернета не было.
- С 1C будут работать только пользователи локальной сети.
- А вот на HTTPS сервер будет лазить много народу с глобальной сети закидывать через него на компьютер USER1 данные которые он будет перенаправлять на SERVER 1c+SQL.
- Все остальные компьютеры должны работать в интернете по определённым адресам, то есть полного доступа не будет.

## 2. Общие данные

### **2.1. Сегментация сети на «внутреннюю» и «внешнюю» или DMZ.**

Основной идеей является разделение сети на несколько сегментов 3-го уровня (сетей и субсетей ) и настройка маршрутизации/фильтрации.

Число сегментов зависит от числа решаемых задач и степени безопасности которую необходимо обеспечить.

Самый простой случай, два сегмента, оно же известно в мире под именем DMZ. Сеть разделяется на оборудование доступное извне и оборудование недоступное извне.

В настоящий момент применяется с двумя оговорками:

- вводится дополнительная фильтрация на вход в сегмент DMZ из Публичной сети (Это не обязательно Internet. Часто может использоваться в Домовых сетях или сложных корпоративных сетях когда в общей MAN/WAN граничат несколько ЛВС).
- В классической схеме DMZ все адреса глобальные, сейчас это роскошь, за сим широко используется NAT.

## 2.2. Сегментация «внутренней» сети по классам оборудования/клиентов.

При требовании защитится не только от внешних, но и от внутренних угроз (или предусмотреть случай «пролома» обороны ) применяется разделение и внутренней сети на сегменты безопасности. Так же данная функция может применяться для обеспечения QoS в сети.

Опять же в простейшем случае применяются всего два сегмента: основной (обычно рабочие станции и сервера общего пользования) сегмент и выделенный сегмент (тут или охраняемое оборудование или основные сервера: SQL, сервера каталогов – в общем при падении коих наступает армагеддец).

Для сегментации возможно применение следующих технологических решений:

- При помощи коммутатора третьего уровня, рис. А.

ЗА: Высокие скорости обмена, отсутствие риска возникновения «узких мест», большое количество сегментов которые возможно создать, относительно невысокая цена при пересчете стоимости порта.

ПРОТИВ: небольшая функциональность фильтрации (по сравнению с фаерволом).

Часто применяют для разгрузки больших сетей от широковещательных запросов и борьбы с «куль-хатцкерами» со снифферами.

ЗЫ: В принципе возможно использование просто интеллектуального коммутатора 2-го уровня ,т. е. настройка фильтрации, но по деньгам выигрыш не так чтоб очень, а производительность и функциональность ниже.

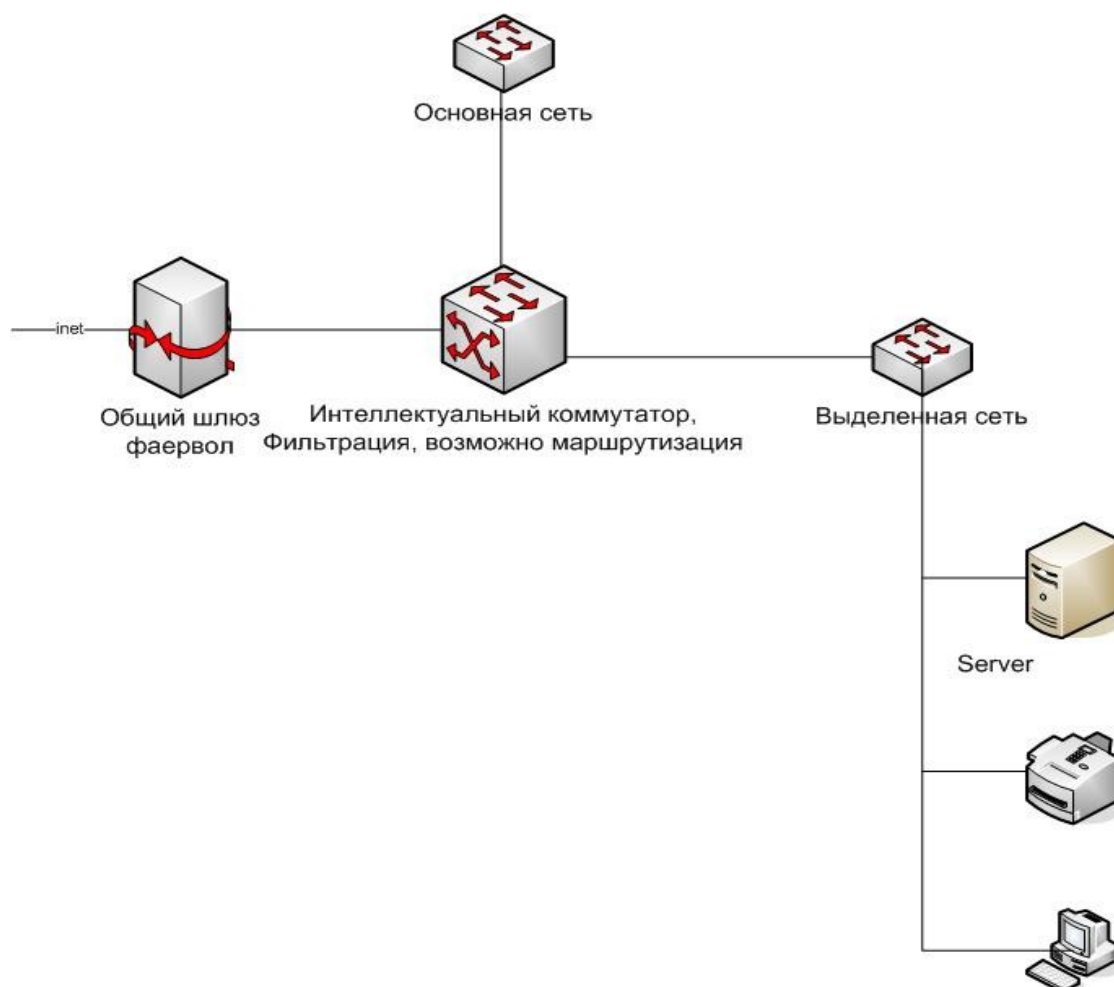


Рис. А. Сегментация при помощи коммутатора 3-го уровня

- При помощи двухвходовых фаерволов (Internet-фаервол), рис. B1, B2.

ЗА: Распространенность устройств, дешевизна, простота настроек через web, относительное богатство настроек прозрачность схемы подключения (для новичка).

ПРОТИВ: невысокие скорости обмена (не смотря на наличие 100 Мбит интерфейсов, обычно данные устройства имеют производительность на обработку порядка 2 Мбит/с – что является типовым значением для интернет-подключений), большой риск возникновения узких мест, громоздкость схемы при большом числе сегментов (синхронное изменение настроек в цепи фаерволов, скажем присмене IP сети – занятие не для слабонервных).

Классическое применение. DMZ в малых сетях – отгораживание WEB и почты.

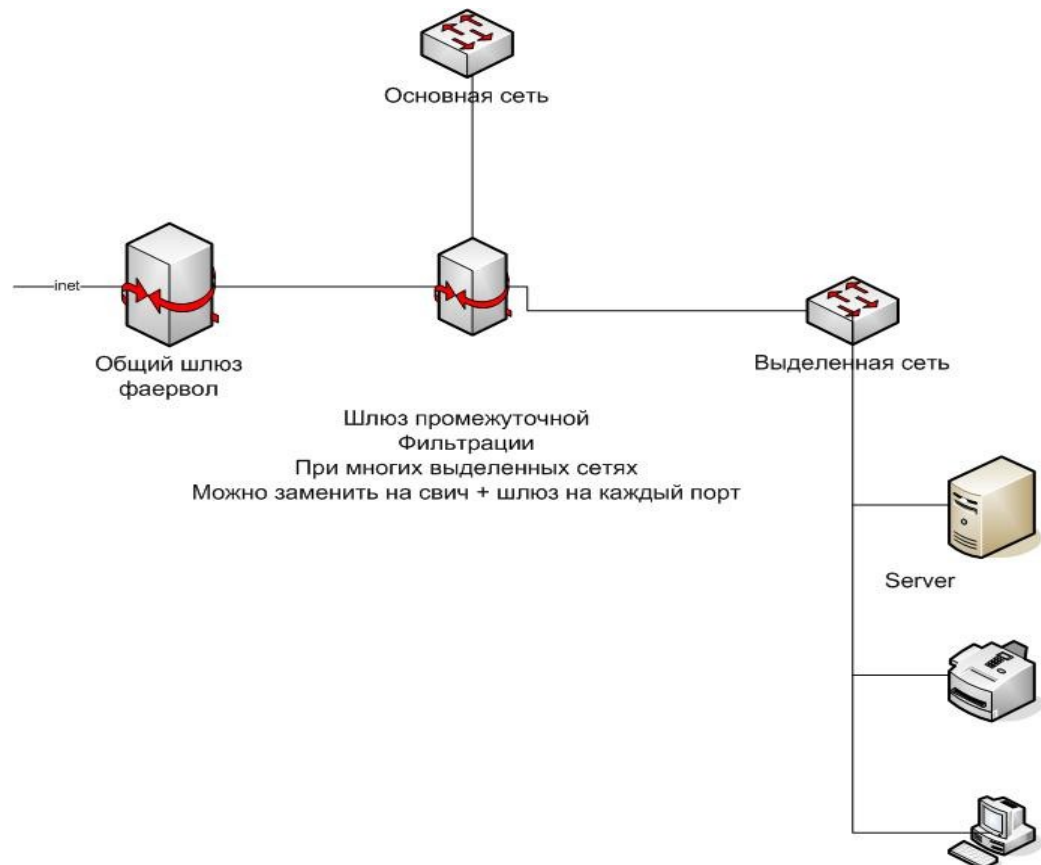


Рис. B1

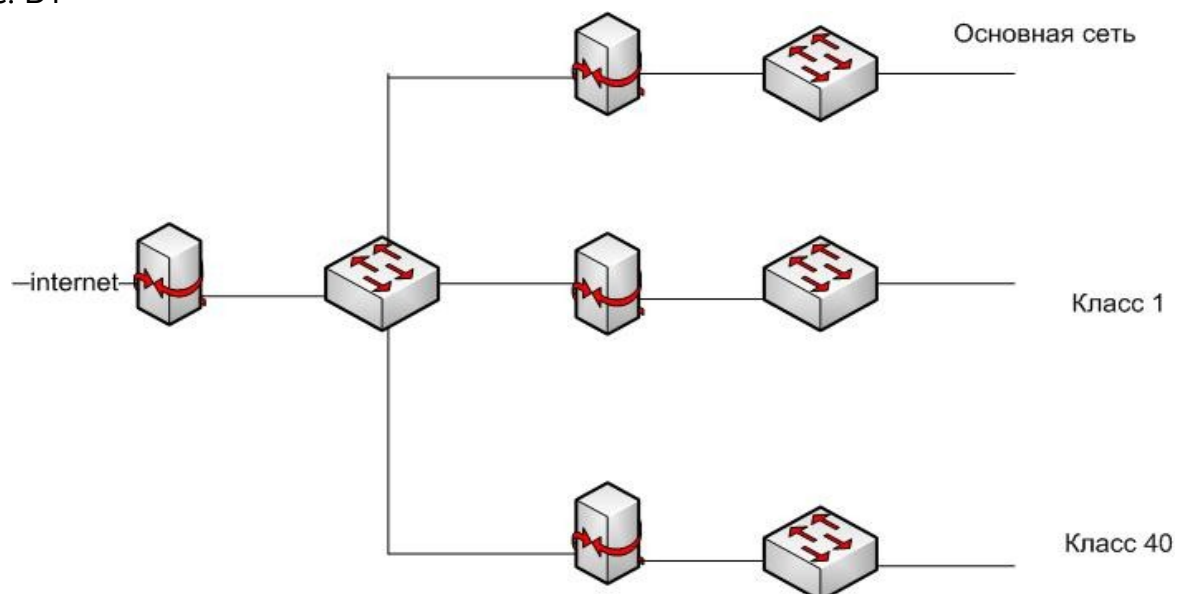


Рис. B2

- При помощи мощных мультивходовых фаерволов + интеллектуальных коммутаторов + VLAN.

ЗА: Высокие скорости обмена (правда все же ниже чем вариант 1), отсутствие риска возникновения «узких мест», большое количество сегментов которые возможно создать, богатство настроек фильтрации.

ПРОТИВ: цена.

Обычно фаервол (маршрутизатор) несколькими физическими интерфейсами объединенными в один логический канал (EtherChannel, LinkAggregation) подключается к интеллектуальному коммутатору. Внутри интерфейс нарезается на виртуальные субинтерфейсы (любое число, равное числу VLAN – сегментов).

Таким образом достигается большая гибкость (число виртуальных субинтерфейсов может быть практически любым и явно больше числа физических интерфейсов фаервола, отказоустойчивость и производительность (весь агрегированный канал в единицу времени может занимать 1 подключение (трафик между активным оборудованием) в случае же отдельного (не агрегированного) подключения интерфейсов - выше скорости интерфейса не прыгнешь).

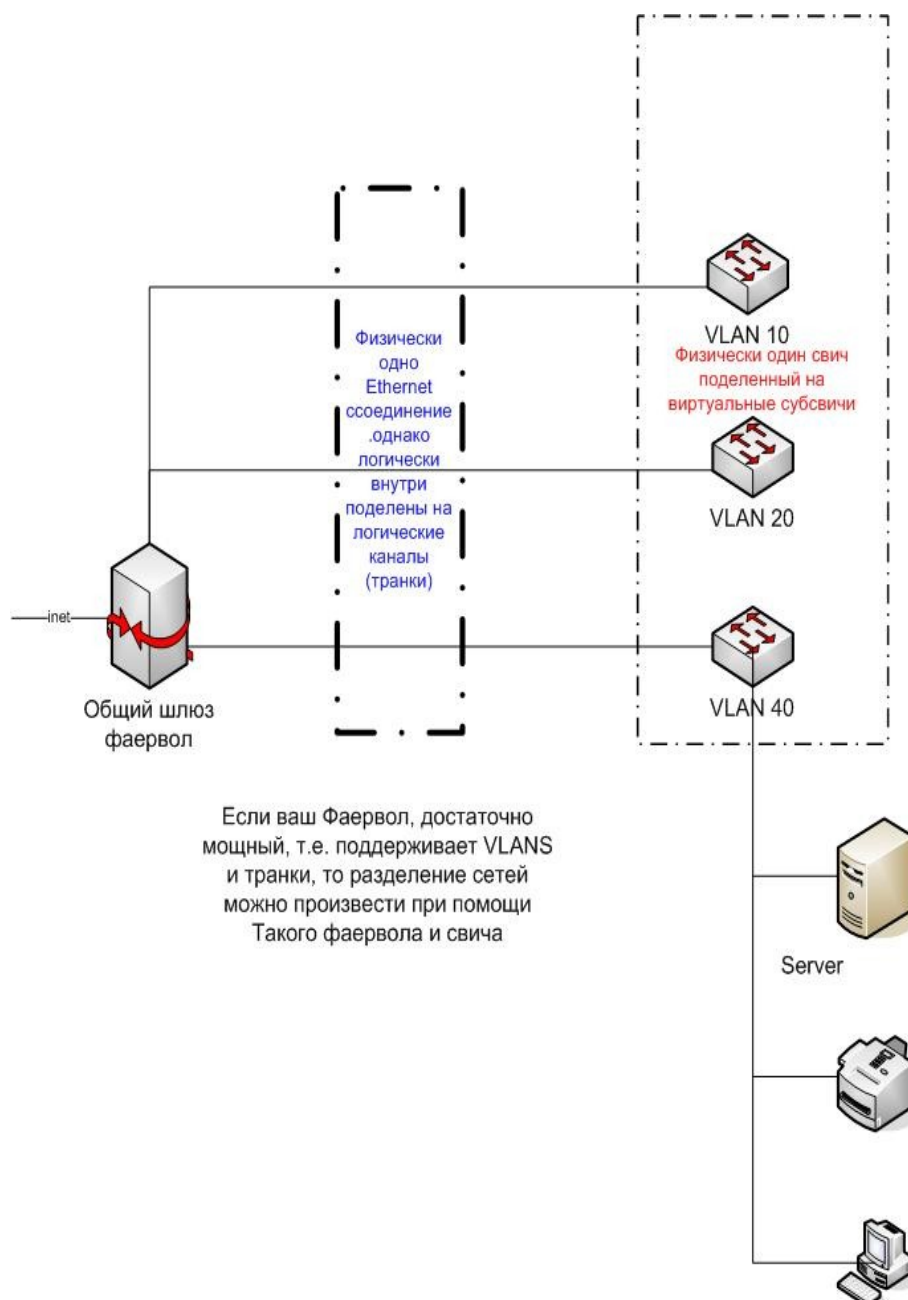


Рис. С.

### 3. Функциональная схема.

#### 3.1. Допущения и ограничения

- × Необходимо одновременное существование 2х интернет провайдеров – с целью резервирования доступа.
- × Не вижу необходимости наличия коммутируемого подключения, т. к. главная задача доступ извне к HTTPS серверу, а ее коммутируемое подключение не решает.
- × Исходя из предыдущих пунктов и общего ТЗ нет необходимости применения маршрутизатора.
- × С целью повышения безопасности и одновременного существования нескольких Internet-соединений предлагается размещение HTTPS-сервера в отдельном сегменте с приватным диапазоном адресов. Доступ HTTPS сервера извне предполагается осуществить при помощи NAT и PORT-MAPPING'a.
- × Наибольшую безопасность предоставит подключение к HTTPS посредством VPN, т. е. полное закрытие всех сервисов от доступа извне.
- × Всего планируется наличие следующих сегментов:
  - Internet 1;
  - Internet 2;
  - HTTPS;
  - Internet Servers (Mail, Proxy, Web);
  - 1C;
  - Servers;
  - Workstation;
  - SuperWorkstation or Admin.

#### 3.2. IP-адресация и VLANs

#	Сегменты	VLAN	IP (mask 255.255.255.0)
1	Internet 1	11	192.168.11.0
2	Internet 2	12	192.168.12.0
3	HTTPS	20	192.168.20.0
4	Internet Servers (Mail, Proxy, Web);	30	192.168.30.0
5	Servers	40	192.168.40.0
6	Workstation	50	192.168.50.0
7	SuperWorkstation or Admin	60	192.168.60.0
8	1C	100	172.1.100.0

- приватный диапазон для интернет сегмента выделен «на всякий»
  - Все что не разрешено явно – запрещено.
  - Для 1С – специально выделен сегмент «не совпадающий» с остальными. дабы можно было ограничить доступ не только при помощи фильтрации, но и при помощи маршрутизации.
  - в сегмент 1с разрешен трафик только из WS сегмента (и возможно SERVERs), желательно ограничить и протокол, скажем только RDP/ICA.
  - Workstation могут ходить в servers, Internet Servers
  - Наружу могут ходить Internet Servers, HTTPS
  - На HTTPS внутри может попасть только Admin
- × Наибольшую безопасность предоставит подключение к HTTPS посредством VPN, т. е. полное закрытие всех сервисов от доступа извне.

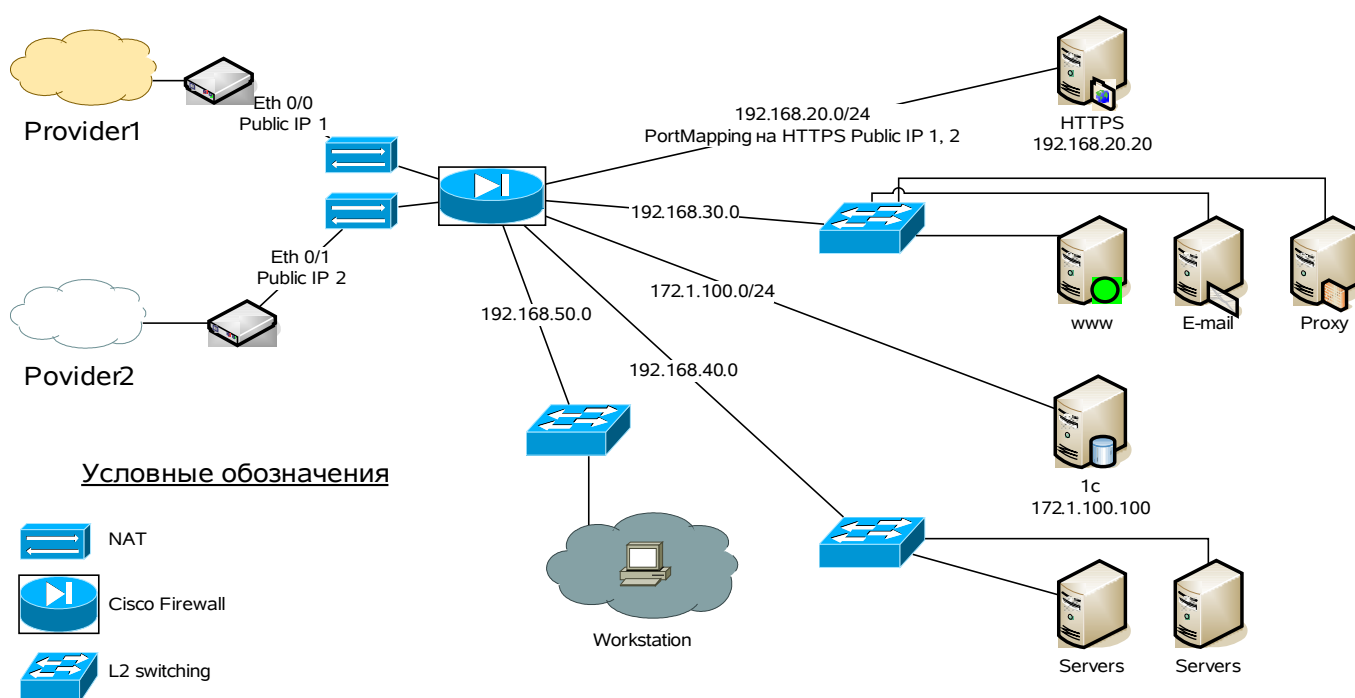


Рис. 4. Функциональная схема Cisco Firewall

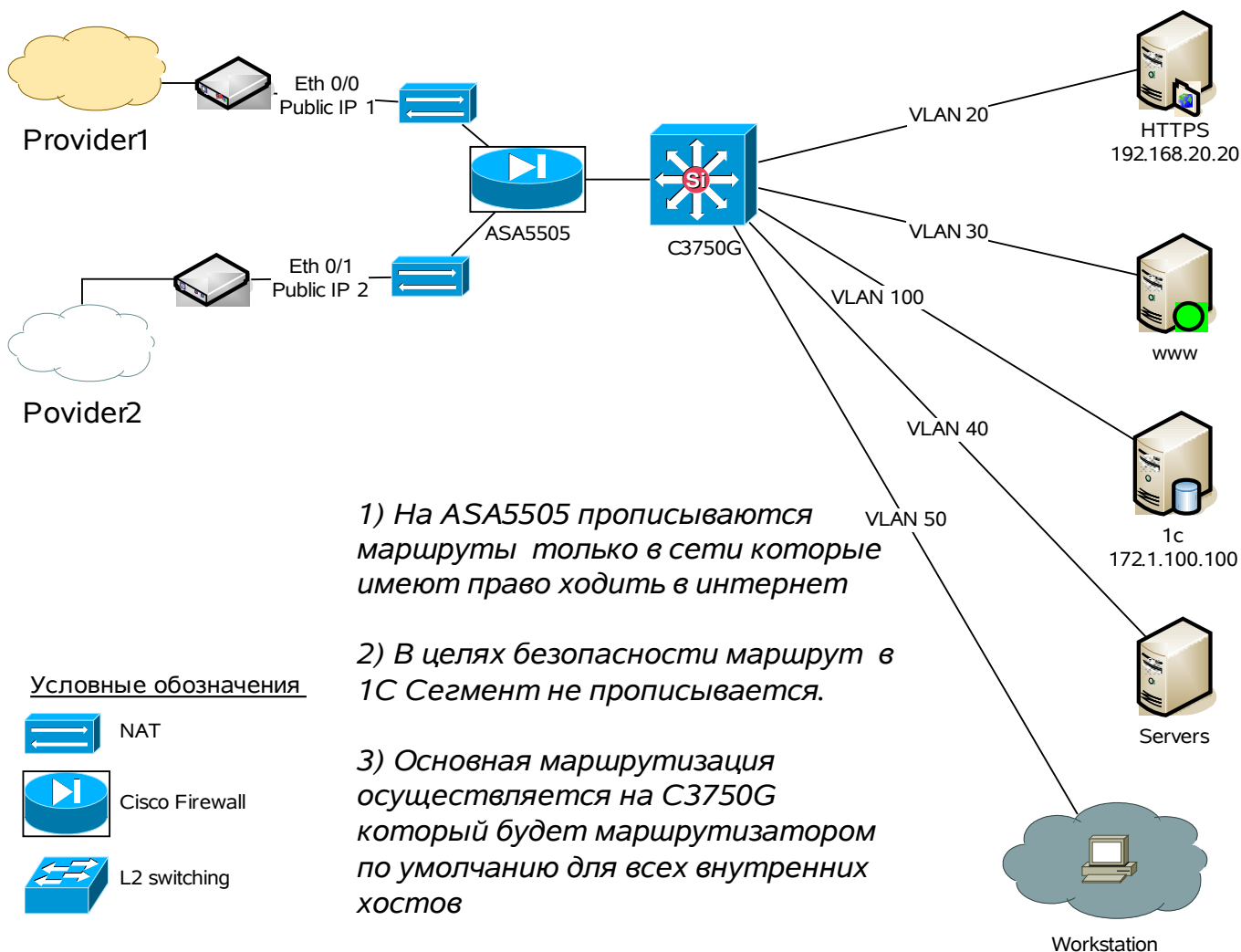


## 4. Решения.

### 4.1. Коммутация 3-го уровня

Предлагаемое оборудование.

#	что	Модель	Цена	Примечание
1	Коммутатор 3-го уровня	WS-C3750G-24T-S Catalyst 3750 24 10/100/1000T Standard Multilayer Image	4500	
2	Фаервол	ASA 5505 Sec Plus Appliance with SW, UL Users, HA, 3DES/AES (ASA5505-SEC-BUN-K9)	1600	Необходима Security Plus прошивка (лицензия) для задействования функции резервирования провайдеров (в представленной модели она уже есть).



## 4.2. Мощный фаервол + коммутация 2-го уровня+VLANs.

#	что	Модель	Цена	Примечание
1	Коммутатор 2-го уровня	WS-C2960G-24TC-L Catalyst 2960 24 10/100/1000, 4 T/SFP LAN Base Image	2500	
2	Фаервол	ASA5520-BUN-K9 ASA 5520 Appliance w/ SW, 300 VPN Peers, 4GE + 1FE, 3DES/AES	6000	

