Задание №5: настройка ACL и NAT

Вы – администратор сети небольшого предприятия, которое занимается розничной торговлей. Сеть, топология которой представлена на рисунке 1, состоит из следующих элементов:

- 4 VLAN, которые реализованы на сетевых устройствах SwFloor1, SwFloor2, MainSwitch и BorderGW
    - каждая VLAN объединяет устройства из соответствующего структурного подразделения: VLAN “Accounts” обслуживает бухгалтерию, VLAN “Sales” обслуживает отдел продаж, VLAN “HR” обслуживает отдел кадров, VLAN “Management” предназначена для управления сетью
    - сетевые настройки раздаются оконечным устройствам по протоколу DHCP
    - адреса для управления коммутаторами находятся в VLAN “Management”
- Демилитаризованная зона (DMZ), которая реализована на сетевых устройствах BorderGW и SwDMZ
    - в DMZ находятся два сервера (веб-сервер и DNS), которые предназначены как для локального доступа, так и для доступа из Интернет
    - сетевые настройки на этих серверах заданы статически
- Подключение к Интернет
    - провайдер выделил предприятию глобальный адрес 81.17.13.2, который был сконфигурирован на внешнем интерфейсе BorderGW статически
    - на устройстве BorderGW настроен маршрут по умолчанию через внешний интерфейс, Serial 0/0/0

Перед Вами стоит задача наладить доступ внутренних хостов в Интернет и реализовать доступ из Интернет к публичным сервисам предприятия, а также реализовать политику разграничения доступа в сети:

1. Любой хост из Интернет должен иметь возможность зайти на сайт компании по адресу 81.17.13.2. Используйте статический PAT. Для проверки поставьте за маршрутизатором ISP хосты и воспользуйтесь эмуляцией браузера на них.
2. Любой хост из Интернет должен иметь возможность обратиться к DNS-серверу компании по адресу 81.17.13.2. Используйте статический PAT. Для проверки поставьте за маршрутизатором ISP хосты и воспользуйтесь командой nslookup из эмулятора командной строки. Разрешать надо адрес “lvk.cs.msu.su”.
3. Любой хост из внутренней сети должен иметь возможность выйти в Интернет: подключаться по telnet к маршрутизатору ISP, «пинговать» его адрес и т.д. Используйте PAT.
4. Реализуйте политику безопасности:
    a. Обезопасить сегмент для управления сетью:
        i. только хосты из «Management» VLAN могут подключаться для управления к маршрутизатору BorderGW
        ii. внутрь Management VLAN разрешен только обратный трафик.
    b. Изолировать бухгалтерию:
        i. бухгалтерия не должна иметь возможность выхода в Интернет
        ii. никакой хост вне VLAN бухгалтерии не должен иметь возможность подключиться к хостам из этой VLAN.
    c. «Порезать» все лишнее в DMZ:
        i. к хосту WWW разрешен только HTTP и ICMP трафик (в обоих направлениях)
        ii. к хосту DNS разрешен только DNS и ICMP трафик (в обоих направлениях)

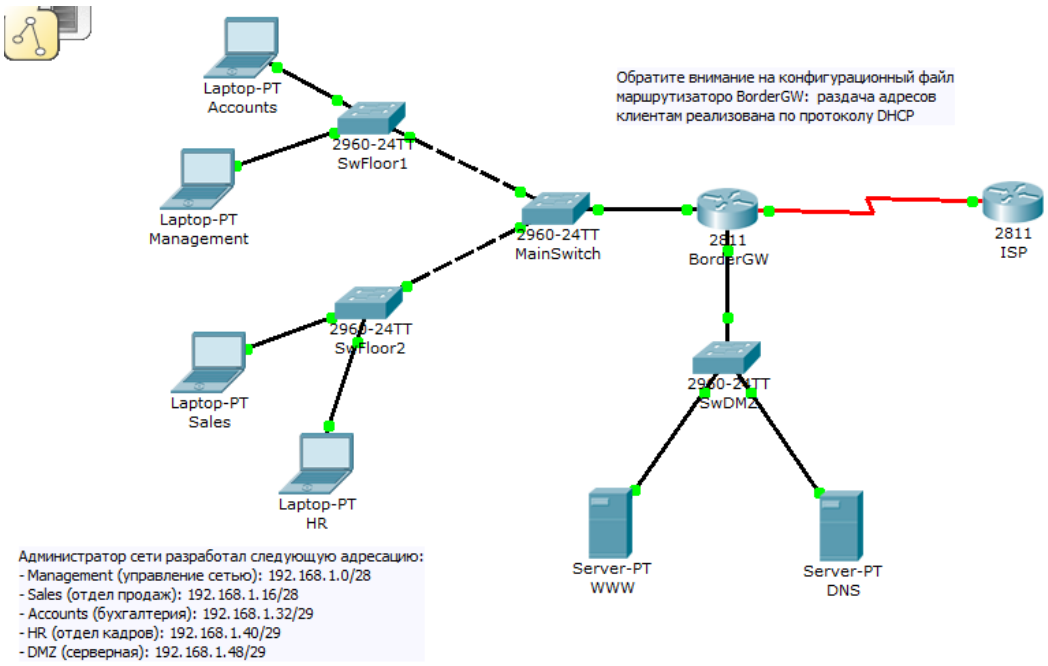

Рисунок 1. Топология сети предприятия.