Дровосеков Д.А. КМБ-16

1. Пояснить рекомендации по настройке механизмов защиты виртуальных ЛВС.

В настоящее время рекомендуется использовать следующие принципы при создании и настройке защищенных коммутируемых ЛВС:

1. **Не использовать для распространения информации об используемых VLAN в ЛВС протокол VTP (включать режим transparent).**

Не позволяет устройства работать с теми VLAN, для работы, с которыми оно не было настроено, т.к. в режиме transparent, устройства не объявляет и не обрабатывает vtp обновления, а передает дальше.

2. **В качестве протокола инкапсуляции использовать протокол IEEE 802.1Q**

IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3 Ethernet. Так как 802.1Q не изменяет заголовки кадра, то сетевые устройства, которые не поддерживают этот стандарт, могут передавать трафик без учёта его принадлежности к VLAN. Поскольку данный стандарт является открытым, он используется для построения "транковых" портов между оборудованием различных производителей. Стандарт применяется для создания защищенных ЛВС.

3. **Запретить передавать кадры собственной VLAN по магистральным каналам. В качестве native VLAN использовать специально для этого выделенную VLAN, не используемую ни для каких других целей.**

Позволяет контролировать трафик, включать только тегированные пакеты.

4. **Не использовать стандартную VLAN 1 в ЛВС ни для каких целей, особенно для управления сетевым оборудованием.**

VLAN 1 включает в себя все порты и принимает весь нетегированный трафик, становиться целью для атаки на устройства.

5. **На магистральных портах использовать только необходимые VLAN – VLAN, которым принадлежат порты коммутаторов на другой стороне. Все другие VLAN запрещать.**

Позволяет усилить контроль за трафиком, не дает возможности несогласованного аппаратного подключения.

6. **Не использовать одинаковые VLAN на разных коммутаторах. Наиболее предпочтительный вариант проектирования – один коммутатор, одна VLAN, одна IP-подсеть.**

Предотвращает коллизию между одинаковыми VLAN и непредсказуемую маршрутизацию трафика, упрощает структуру сети.

7. **Все неиспользуемые порты коммутатора переводить в режим shutdown и назначать их в специально созданную для этого немаршрутизируемую и изолированную VLAN.**

Позволяет контролировать трафик, включать только тегированные пакеты.

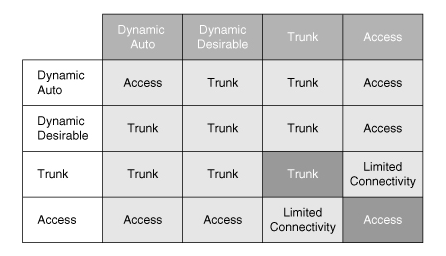
8. **На портах доступа отключать использование протокола DTP. Для минимизации времени восстановления функционирования системы при подключении канала на магистральных портах устанавливать протокол DTP в режимах On/On и Nonegotiate (отключать согласование).**

Исключает возможность подключения к сети злоумышленники через access порт.

2. Реализовать в ЛВС атаку типа «VLAN hopping» при настройке различных собственных VLAN на транковых портах, соединяющих коммутаторы.

Атака VLAN hopping базируется на возможности коммутаторов автоматически согласовывать тип своего порта - access или trunk. Используется для этого проприетарный протокол компании Cisco DTP (Dynamic Trunking Protocol). При его использовании (а он включен по умолчанию) возможны следующие состояния порта: dynamic auto, dynamic desirable, static access, static trunk.

Согласования состояния двух портов, подключенных друг к другу:



При определенных условиях, а именно в режимах dynamic auto и dynamic desirable порт коммутатора может согласовать свою работу в режиме trunk. Это значит, что если атакующее устройство будет вести себя как порт в режиме desirable оно согласует на себя trunk-порт и получит доступ к трафику всех VLAN’ов, которыми оперирует коммутатор.

Основная проблема заключается в том, что на коммутаторах Cisco все порты по умолчанию находятся в режиме auto. Поэтому даже если порт настроен в режиме access/auto при получении запроса на согласование его состояние может измениться на trunk/auto.

3. Настроить распространение базы данных VLAN через протокол VTP в соответствии с рекомендуемыми параметрами.

Рекомендуемые параметры: **Не использовать для распространения информации об используемых VLAN в ЛВС протокол VTP (включать режим transparent).**

После выполнения поставленных задач коммутаторы SW4-1, SW4-2 и SW4-3 будут находиться в режиме transparent, и не будут объявлять и обрабатывать приходящие vtp-обновления, но при этом все приходящие обновления будут передаваться дальше.

4. Настроить терминирование и маршрутизацию VLAN на коммутаторе уровня ядра-распределения ЛВС.

Данные настройки производятся на шаге №5