Защита инфраструктуры

Teach
Me
Skills

Собираемся и отмечаемся

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. **Для чего необходим DHCP?**
2. **Что такое демоны в linux?**
3. **В чем отличие firewall, брандмауэра и сетевого экрана?**
4. **Что такое syslog?**

Mini-quize по новой теме:

1. **Как вы думаете, может ли AD работать с unix-like системах?**
2. **В чем отличия прокси и VPN?**
3. **Как вы думаете, что такое SNMP-trap?**
4. **Что такое ADDS?**
5. **Зачем DNS в ADDS?**
6. **Что такое привелегия?**

Teach Me Skills

План занятия

1. Рассмотрим отличия Windows user-edition и Windows server
2. Изучим причины создания AD и как оно работает
3. Разберемся с брандмауэрами
4. Рассмотрим portsecurity и dot1x
5. Разберемся зачем zero trust в инфраструктуре и как его применяют
6. Рассмотрим различные тактики защиты периметра

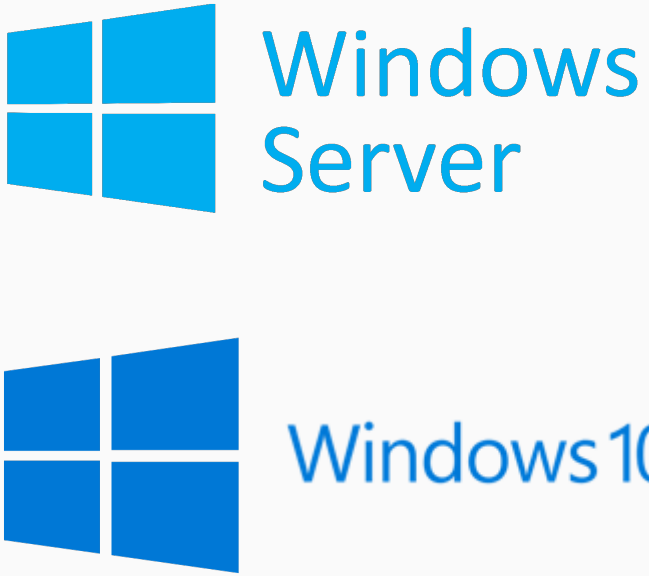
Windows Server

Windows Server — линейка серверных операционных систем от компании Microsoft.

Отличия от обычной версии:

1. **Серверная версия имеет расширенный функционал ядра (пользователи, больший пул ресурсов).**
2. **Серверная версия может работать без gui управляясь через powershell.**
3. **В серверной стоит доп. ПО для администрирования.**
4. **В персональной версии стоит различное пользовательское ПО.**

Выпуск версии серверной ОС относится к каждой версии обычной ОС.



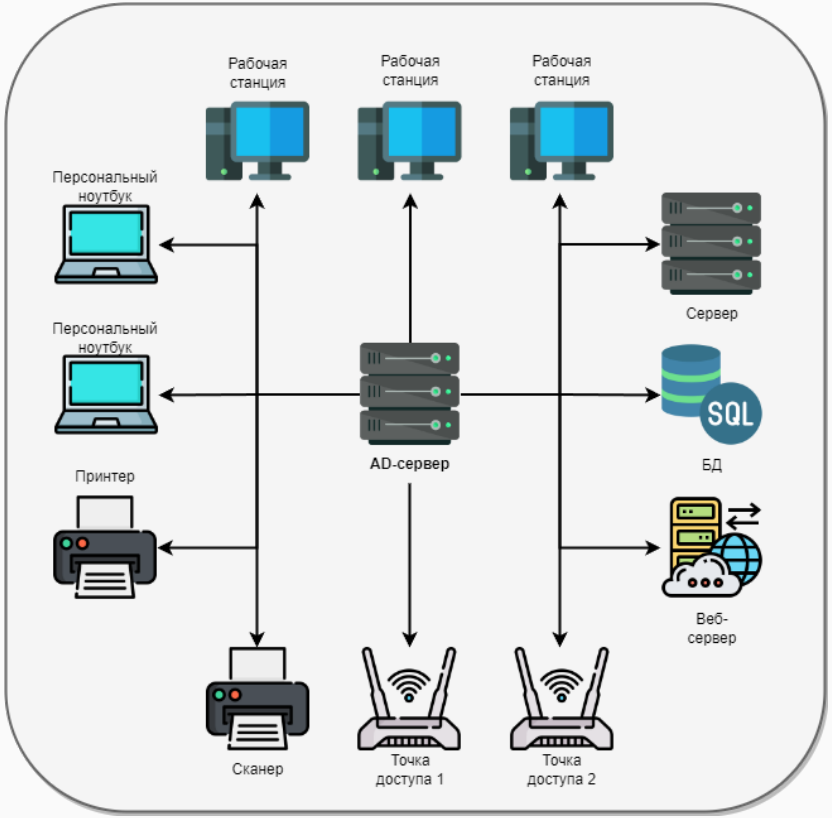
ActiveDirectory

Active Directory — службы каталогов для операционных систем семейства Windows Server. Создавалась, как LDAP-совместимая реализация службы каталогов. Хранит данные и настройки среды в централизованной базе данных.
Начиная с WinServer 2008, включает возможности интеграции с другими службами.

- Позволяет администраторам использовать групповые политики,
- разворачивать программное обеспечение на множестве,
- устанавливать обновления операционной системы.

Сети Active Directory расширяемые.

Релизнулась в 99-ом, платформы x86, x86-64, IA-64



ActiveDirectory#2

ADDS –Active Directory Domain Services

Inbound/outbound replication
RPC или **SMTP**

Безопасность

Регулярные бэкапы

Удобный обмен файлами

Единая место аутентификации

Удобное управление политиками

Интеграция сервисов и оборудования

Наличие дублирующего контроллера доменов

Single sign-on - технология единого входа

Роли WindowsServer

Роль сервера – набор ПО, позволяющего компьютеру выполнять определенную функцию для пользователей или других компьютеров в сети

Файловый сервер

Сервер печати

Сервер приложений

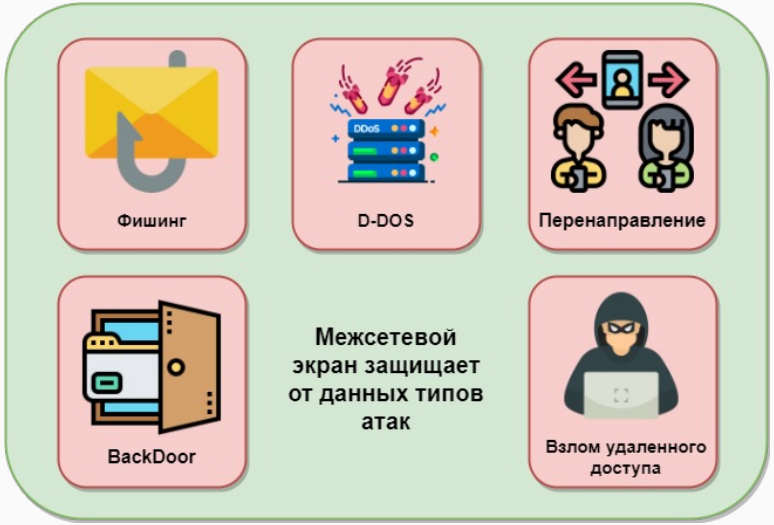
Веб-сервер

DNS-сервер и DHCP-сервер

Службы в Windows Server

Брандмауэры

Брандмауэр — защитный экран между глобальным интернетом и локальной сетью организации. Выполняет функцию проверки и фильтрации данных, поступающих из интернета.



Первые устройства, выполняющие функцию фильтрации сетевого трафика, появились в конце 1980-х. **Маршрутизаторы** инспектировали трафик на основании данных, содержащихся в заголовках протоколов сетевого уровня. Впоследствии они получили возможность выполнять фильтрацию трафика, используя данные протоколов более высокого, транспортного уровня.

Программные межсетевые экраны появились существенно позже чем антивирусы.
Проект **Netfilter/iptables** был основан в 1998 году.

Брандмауэры / Управляемые коммутаторы

Управляемые коммутаторы - причисляют к классу межсетевых экранов, так как они осуществляют фильтрацию трафика между сетями или узлами сети.
Они работают на **канальном уровне** и разделяют трафик **в рамках локальной сети**, и не могут быть использованы для обработки трафика из внешних сетей.
Фильтруют трафик на основе **MAC-адресов**, содержащихся в заголовках фреймов.
В коммутаторах семейства **Cisco** эта возможность реализована при помощи механизма **Port Security**.

Достоинства:
Мощное и дешёвое решение.
Высокая скорость.
Недостаток:
невозможность анализа протоколов более высоких уровней

Брандмауэры / Пакетные фильтры

Пакетные фильтры функционируют **на сетевом уровне** и контролируют прохождение трафика на основе информации в заголовке пакетов.

Межсетевые экраны данного типа могут оперировать заголовками протоколов транспортного уровня. **Фильтры реализованы** в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах.
При анализе заголовка пакета используются следующие параметры:
•**IP-адреса** источника и получателя;
•**тип протокола**;
•**поля служебных заголовков** протоколов;
•**порт** источника и получателя.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры:
•пограничные маршрутизаторы;
•операционные системы;
•персональные межсетевые экраны.

Достоинства:	Недостатки:
Быстрая работа	**Невозможность анализировать протоколы высоко уровня**

Брандмауэры / Шлюзы сеансового уровня

Шлюз сеансового уровня **исключает** прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая **в качестве прокси**, который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения.

Шлюз сеансового уровня гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению.

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создаёт видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети.

Достоинства: эффиктивная защита от аттак.
Недостатки: отсутствует возможность проверки данных.

Брандмауэры / Инспекторы состояния

Все достоинства предыдущих устройств совмещает в себе **инспектор состояния** – осуществляющий фильтрацию трафика с сетевого по прикладной уровень.
Он позволяет контролировать:
каждый передаваемый пакет — на основе таблицы правил;
каждую сессию — на основе таблицы состояний;
каждое приложение — на основе разработанных посредников.

Достоинства:
Производительность на уровне пакетных фильтров.
прозрачность для пользователя,
большие возможности расширения.

Недостатки:
более низкая защищённость.

Port security

Port security — функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. Если MAC-адрес отправителя не указан как разрешенный, данные не будут переданы

Режимы запоминания MAC-адресов:
Continuous — без ограничений.
Static — от 0 до 8 статических MAC, остальные - динамически получены.
Configured — от 1 до 8 статических MAC, динамические – запрещены.
Limited-continuous — от 1 до 32 динамических MAC.
Port-access — использует 802.1 для временного получения MAC сессии 802.1X.

Port security#2

Нарушение безопасности:
Максимум безопасных MAC было добавлено в таблицу, и хост не из таблицы, пытается получить доступ.

Cisco/ProCurve
Режимы реагирования :
Protect (none) — кол-во безопасных MAC - максимально, пакеты – отбрасываются, пока не будет места в таблице.
Оповещения о нарушении безопасности нет.

restrict (**send-alarm)** — кол-во безопасных MAC – максимально, пакеты - отбрасываются, пока не будет места в таблице.
В при нарушении отправляются **SNMP trap** и сообщение **syslog**.

Shutdown (ыend-disable) — интерфейс переводится в заблокированное состояние и выключается немедленно. Отправляются **SNMP trap** и сообщение **syslog**.

Data diode

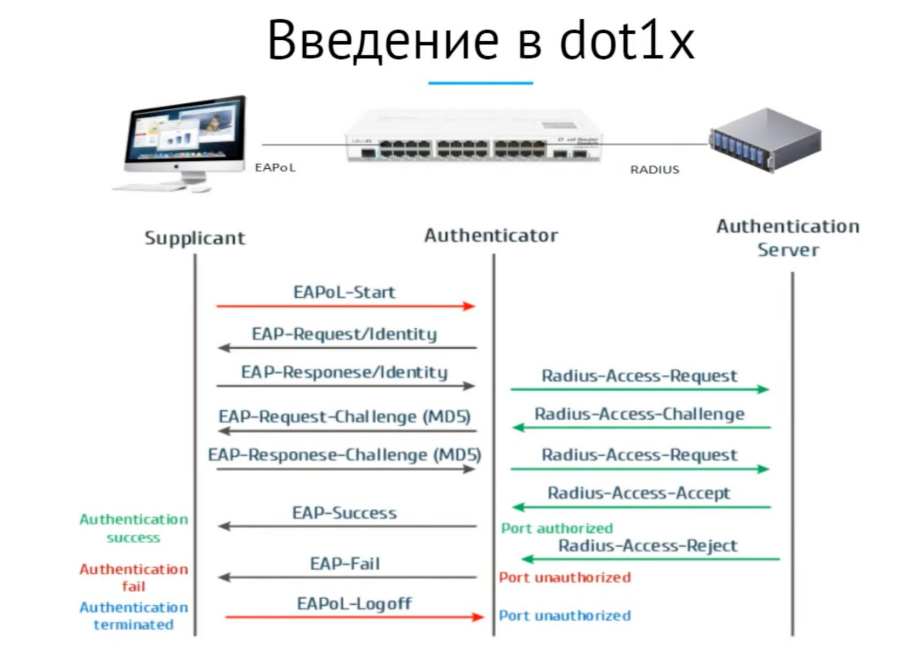
Однонаправленный шлюз или **диод данных** — устройство, которое позволяет данным перемещаться только в одном направлении, передача данных в другом направлении физически невозможна.

Позволяет создавать **системы недоступные для воздействия извне**, но при этом **допускающие сбор данных** — например, с датчиков или различных логов.

Позволяет **предоставить безопасный доступ** к критически важной системе путём её **реплицирования**. Пользователь при этом работает с копией важного хоста, не имея возможности **нанести вред** исходному серверу.

Dot1x

Протокол Dot1x — это технология защиты Локальной сети организации от подключения сторонних устройств.



Преднастройки: Настройка Windows Server

Что необходимо для запуска dot1x

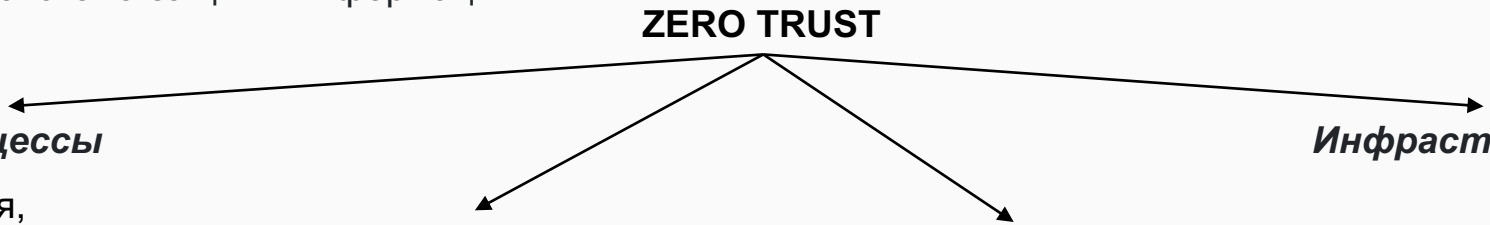
- Active Directory
- NPS
- Центр сертификации (Можно без него при авторизации через логин/пароль)

Порядок действий

- Генерируем сертификат
- Создаем учетную запись в AD и привязываем к ней открытый сертификат
- Переносим сертификат в контейнер компьютера
- Настраиваем сетевую карту на клиенте для работы с 802.1x

Опять ZeroTrust?

Zero Trust – это подход к созданию системы информационной безопасности, который предполагает отсутствие доверия по умолчанию.
СЗИ – система защиты информации



Процессы

Действия, направленные на постоянную проверку и аутентификацию, а так же на предоставление минимального доступа.

СЗИ

К ним относятся различные устр-ва обеспечивающие выполнения процессов. Так же инструменты анализа и прочие решения.

Персонал

Люди так же должны использовать данный подход для обеспечения защиты от соц.инженерии.

Инфраструктура

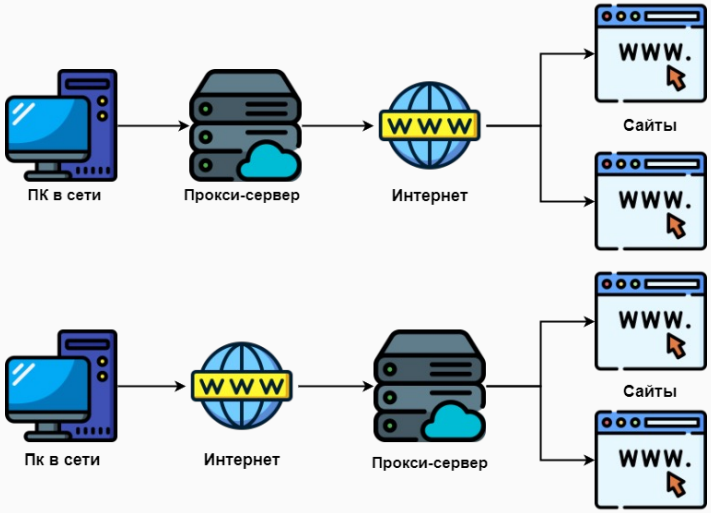
Инфраструктура должна позволять реализовывать различные методики ZeroTrust. Иначе, нет смысла заниматься внедрением подхода.

Zero trust#2

Нобходимо доверять своим пользователям.

Прямой прокси

Прямой прокси, это сервер, который находится перед группой клиентских компьютеров.



Обратный прокси находится прямо перед веб-сервером.

- **Прокси позволяет** избежать ограничений в отдельно взятой стране или для компьютеров внутри организации. Обойти ограничения брандмауера.
- **Прокси позволяет** ограничить доступ к тому или иному контенту.
- **Прокси позволяет** сохранять анонимность.

Reverse Proxy

Обратный прокси позволяет:

Балансировать нагрузку. Например, сайт, не справиться с нагрузкой и не сможет обрабатывать весь трафик с помощью одного сервера. В таких случаях трафик можно распределить по нескольким веб-серверам.

Защита от атак. Обратный прокси позволяет исходным серверам не раскрывать свои IP адреса клиентам

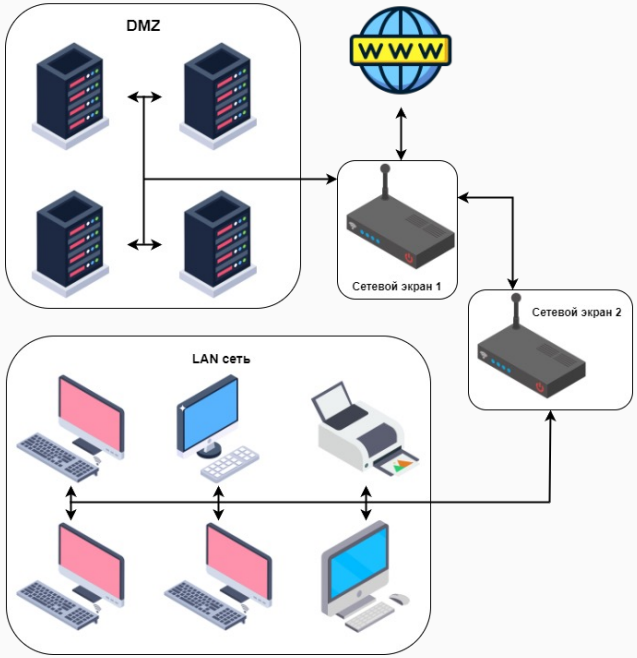
Глобальная балансировка нагрузки на сервер. распределение сайта по нескольким серверам, которые физически расположенны в разных странах мира. Обратный прокси отправляет запрос пользователя на сервер, который географически находится ближе к нему.

Кэширование. Обратный прокси-сервер также может кэшировать содержимое запроса и таким образом повышать производительность.

SSL-шифрование. Шифрование и дешифрование сообщений (SSL или TLS) для каждого клиента по отдельности тяжело в плане вычислений для исходного сервера. Обратный прокси-сервер можно настроить для расшифровки всех входящих запросов и шифрования всех исходящих ответов, освободив ресурсы на исходном сервере.

DMZ

DMZ — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.



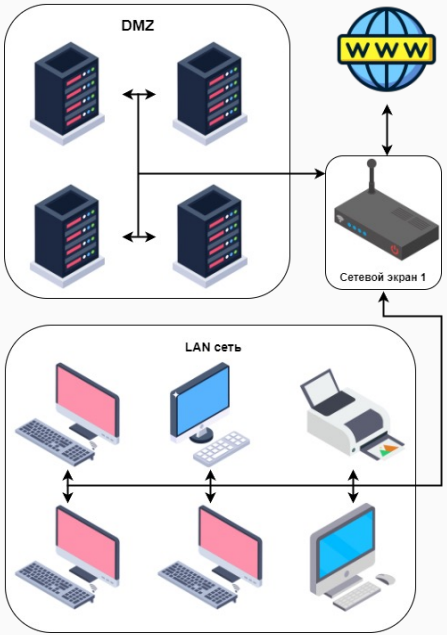
DMZ с 2-мя сетевыми экранами

контроль доступа из внешней сети в ДМЗ

контроль доступа из внутренней сети в ДМЗ

контроль доступа из внутренней сети во внешнюю

запрет доступа из внешней сети во внутреннюю



DMZ с 1-мя сетевыми экранами

IDM

IDM Identity Management –
комплекс подходов, технологий и специальных программных средств для управления учётными данными пользователей.

Автоматическое получение данных о пользователе,
Централизованное управление **политиками**,
Централизованное управление **учетными данными**,
Централизованное управления **процессами пользователя**,
Централизованное управление **группами**, **обновление** и т.д

Достоинства:
Автоматизированное управление
Экономия времени
Единая точка регистрации и аудита
Повышение защищенности

PIM

PIM
Privileged Identity Management – управление тем, какие ресурсы могут использовать привелегированные пользователи.

PAM

PAM Privileged Account Managment –
управление привелегированным доступом.

Привилегия – полномочие,
которое учетная запись или
процесс имеет
в вычислительной системе.

Включать в себя разрешения на выполнение следующих действий:

- выключение систем,
- загрузка драйверов устройств,
- настройка сетей или систем,
- подготовка и настройка учетных записей,
- подготовка и настройка облачных экземпляров и т. п.

Teach
Me
Skills

Спасибо за внимание!