**Основы управления доступом и резервного копирования в сетях**

## Управление пользователями и доступом

**Управление пользователями и доступом (Identity and Access Management, IAM)** — это комплексная система, которая охватывает многие процессы и позволяет организации управлять идентификацией пользователей и их доступом к различным ресурсам.

Некоторые функции систем IAM:

* ***Управление учётными записями (User Administration and Provisioning, UAP)***. Такие системы позволяют управлять идентификационными данными, паролями, производить интеграцию с кадровыми системами. UAP проверяет заполнение всех атрибутов пользователя в соответствии с правилами и запрещает создание некорректных записей.
* ***Управление доступом (Identity Access Management, IAM).*** Такие системы предоставляют возможности по контролю полномочий сотрудников при обращении к веб-ресурсам, выявлять и предотвращать несанкционированный доступ, производить аудит активности сотрудников и блокировать попытки мошенничества.
* ***Управление удостоверениями (Identity and Access Governance, IaG).*** Такие системы позволяют гибко управлять правами доступа к приложениям, сервисам и данным (роли, полномочия, правила, политики доступа), автоматизировать процессы согласования предоставления прав доступа, обнаруживать конфликты полномочий и управлять рисками.
* ***Обеспечение единого доступа (Enterprise Single Sign-On, SSO).*** Системы IAM могут предоставлять возможность настройки централизованной аутентификации сотрудников, которые используют корпоративные приложения. При использовании таких систем пользователю не требуется многократно вводить пароль, если требуется войти в несколько различных систем.

Роли устанавливают права доступа пользователя к записям модулей системы. При помощи ролей можно ограничивать права на просмотр, редактирование, удаление записей, а также права на импорт и экспорт записей конкретному пользователю (либо группе пользователей) в рамках определённого модуля.

Пароли используются для идентификации и проверки подлинности пользователей. Для повышения безопасности часто используется многофакторная аутентификация, где идентификационные данные состоят из нескольких факторов, таких как пароль и биометрические данные.

## Ролевая Модель управления доступом

**Ролевая модель управления доступом** (RBAC) — это подход к управлению правами доступа пользователей к ресурсам системы, основанный на их ролях.

Вместо назначения прав каждому пользователю точечно, права доступа группируются по ролям, а пользователи получают доступ к ресурсам уже в зависимости от своей роли. Это упрощает управление доступом и снижает вероятность ошибок при назначении прав.

Основные компоненты RBAC:

* Роли – логические объединения прав доступа, соответствующие определенным обязанностям или функциям в организации;
* Пользователи – субъекты, которым назначаются определенные роли;
* Права доступа – разрешения на выполнение определенных действий с ресурсами системы;
* Ресурсы – объекты системы, к которым необходимо управлять доступом (файлы, базы данных, приложения и т.д.).

Назначая пользователям роли, организация контролирует их доступ к ресурсам и функциям системы, обеспечивая соответствие их обязанностям и уровню ответственности.

Основные этапы работы модели:

* ***Определение ролей:*** анализируются функции сотрудников и их должностные обязанности, на основе чего создаются соответствующие роли с необходимыми правами доступа;
* ***Назначение ролей пользователям:*** каждому пользователю присваивается одна или несколько ролей в зависимости от его должностной инструкции;
* ***Назначение прав ролям:*** каждой роли присваиваются строго определенные права доступа;
* ***Контроль доступа:*** при попытке пользователя получить доступ к тем или иным ресурсам система проверяет его роли и соответствующие им права, разрешая доступ или запрещая его.

## Системы аутентификации, авторизации и управления аккаунтами

**Аутентификация, авторизация и учёт** (AAA) – это система и методология, используемые для обеспечения безопасности и контроля доступа к информационным ресурсам в компьютерных сетях.

Компоненты модели ААА:

* Аутентификация (authentication) - это проверка личности пользователя, который пытается получить доступ к сети или сетевому устройству. Обычно для этого используются логин и пароль, но могут быть и другие методы, такие как сертификаты, смарт-карты или биометрия;
* Авторизация (authorization) - это определение прав и ограничений пользователя в сети. Например, какие ресурсы он может использовать, какие команды он может выполнять, какие данные он может видеть и т.д;
* Учёт (accounting) - это запись и отслеживание информации о действиях пользователя в сети. Например, когда и сколько времени он был подключен, сколько трафика он передал или получил, какие ресурсы он использовал и т.д.

Для реализации AAA в сетях обычно используются специальные серверы доступа, которые обрабатывают запросы от сетевых устройств или клиентов.

## Список контроля доступа ACL

**Список контроля доступа** (ACL) — это функция сетевой безопасности, которая действует как фильтр или набор правил, применяемых к сетевому интерфейсу, маршрутизатору или брандмауэру.

ACL определяет, какой сетевой трафик разрешён или запрещён, основываясь на различных параметрах:

* IP-адреса источника и назначения;
* номера портов;
* протоколы;
* другие критерии, заданные сетевым администратором.

Основная цель ACL — повысить безопасность путём ограничения или разрешения доступа к различным компонентам системы: файлы, каталоги, устройства, сетевые порты и службы.

Типы ACL:

* ***Стандартные.*** Основаны исключительно на IP-адресе источника трафика. Простые и менее детализированные, но могут быть полезны в определённых сценариях, где требуется фильтрация только IP-адреса источника;
* ***Расширенные.*** Обеспечивают большую гибкость, позволяя создавать правила на основе IP-адресов источника и назначения, протоколов, номеров портов и других параметров. Подходят для сложных сетевых сред;
* ***Рефлексивные.*** Проводят фильтрацию трафика с помощью данных сеанса верхнего уровня. Работают с помощью TCP-запросов и ответов;
* ***Динамические.*** Дают системным администраторам возможности предоставить пользователю временный доступ или ограничить доступ к маршрутизатору из интернета.

ACL могут быть размещены на различных сетевых устройствах. Например, на маршрутизаторах для контроля трафика между различными сетями или подсетями, или на уровне коммутатора для защиты доступа к его управлению или контролю трафика между различными VLAN.

Виды фильтрации ACL:

Фильтрация трафика в ACL (списке контроля доступа) происходит на основе заданных критериев. Эти критерии могут включать IP-адреса, номера портов и протоколы.

ACL работает последовательно: пакеты проверяются на соответствие каждому правилу в списке, пока не будет найдено совпадение. Если совпадение не найдено, применяется действие по умолчанию.

***Фильтрация по IP адресу:*** в ACL можно указать правило, которое будет действовать на трафик с определённым IP-адресом. Для этого в списке доступа используется атрибут host или any. Например, правило может разрешать или запрещать трафик с IP-адресом конкретного хоста или всей подсети.

***Фильтрация по портам:*** в ACL можно указать правило, которое будет действовать на трафик с определённым портом или диапазоном портов. Для этого в списке доступа используется атрибут eq (равен) или neq (не равен). Например, правило может разрешать или запрещать трафик на конкретном порте или в определённом диапазоне.

***Фильтрация по протоколам***: в ACL можно указать правило, которое будет действовать на трафик с определённым протоколом. Для этого в списке доступа используется атрибут protocol. Например, правило может разрешать или запрещать трафик по протоколу TCP, UDP, ICMP.

Реализация ACL:

Внедрение ACL включает в себя следующие шаги:

* Определите задачи и цели внедрения ACL. Обозначьте конкретные сетевые ресурсы, которые нуждаются в защите и определите желаемые политики контроля доступа;
* Проанализируйте схемы сетевого трафика для выявления потенциальных уязвимостей безопасности и областей, требующих контроля доступа. Этот анализ поможет в определении соответствующих правил ACL;
* Создайте правила ACL на основе выявленных требований. Рассмотрите тип ACL и определите необходимые параметры;
* Протестируйте правила ACL в контролируемой среде, прежде чем развертывать их в производственной сети. Убедитесь, что правила работают так, как задумано, и не вызывают никаких непредвиденных последствий или сбоев.

## Резервное копирование и восстановление

Резервное копирование конфигураций сетевых устройств (маршрутизаторов, коммутаторов) — критически важная процедура, позволяющая быстро восстановить работоспособность системы после сбоев, ошибок администрирования или аппаратных отказов. Резервные копии сохраняют:

* Настройки интерфейсов;
* Таблицы маршрутизации;
* Параметры безопасности (ACL, пароли);
* Конфигурации протоколов (OSPF, VLAN и др.).

Некоторые задачи сетевого администратора при построении системы резервного копирования:

* анализ данных, используемых компанией, и определение степени их критичности для деятельности компании;
* определение объёмов данных, подлежащих архивированию, и интенсивности их модификации;
* разработка стратегии резервного копирования каждого типа информации;
* создание и настройка заданий для выполнения резервного копирования;
* регулярный просмотр журналов, в которые записываются протоколы резервного копирования;
* регулярное тестирование созданных резервных копий.

Существуют определенные программы для резервного копирования, которые помогают автоматизировать процесс сохранения и восстановления конфигураций сетевых устройств и данных:

* **Acronis True Image**. Популярная программа для резервного копирования данных, подходит для домашнего использования и малого бизнеса. Позволяет делать резервные копии не только отдельных файлов, но и целых жёстких дисков;
* **Handy Backup**. Программа для резервного копирования и восстановления данных ПК. Поддерживает полное, дифференциальное, инкрементное или смешанное копирование, а также резервное копирование баз 1С и СУБД;
* **RuBackup**. Российская система резервного копирования. Обладает встроенной отказоустойчивостью, совместима с отечественными ОС, имеет модульную архитектуру и открытый API для разработки модулей резервного копирования и восстановления.

Методы резервного копирования и восстановления конфигурации

1. Локальное копирование:

* На устройство:

Сохранение текущей конфигурации в энергонезависимую память NVRAM: ***copy running-config startup-config***

Эта команда сохраняет текущую рабочую конфигурацию (running-config) в постоянную память устройства (startup-config), что позволяет восстановить настройки после перезагрузки.

* На внешний носитель:

Копирование конфигурации на TFTP-сервер: ***copy running-config tftp://192.168.1.100/backup.cfg***

Для выполнения этой команды необходимо иметь настроенный TFTP-сервер по указанному IP-адресу. Альтернативно можно использовать USB-накопитель, если устройство поддерживает такую возможность.

1. Удаленное копирование:

* FTP/SCP:

Безопасное копирование через SCP: ***copy running-config scp://user@server/backup.cfg***

SCP (Secure Copy Protocol) предпочтительнее FTP, так как обеспечивает шифрование передаваемых данных. Требует предварительной настройки SSH-доступа.

1. Облачное хранение:

Для крупных корпоративных сетей целесообразно использовать специализированные облачные платформы управления конфигурациями, которые обеспечивают централизованное хранение, контроль версий и автоматизированное развертывание резервных копий.

1. Восстановление конфигурации:

* Из NVRAM:

Загрузка сохранённой конфигурации в оперативную память:

***configure terminal***

***copy startup-config running-config***

После выполнения этих команд устройство начнёт работать с восстановленными настройками без необходимости перезагрузки.

* С внешнего сервера:

Восстановление с TFTP-сервера: ***copy tftp://192.168.1.100/backup.cfg running-config***

Аналогичная команда доступна для SCP/FTP. Важно убедиться в совместимости версий ПО.

* Полный сброс:

При отсутствии резервных копий может потребоваться: сброс к заводским настройкам, перепрошивка устройства или ручное восстановление конфигурации

## Обновление прошивок и диагностика

Для обновления прошивок и диагностики сети используются команды ping, traceroute и show commands. Эти инструменты позволяют проверять целостность соединений, определять маршруты пакетов и анализировать данные устройства.

Команда ping

Команда ping отправляет пакеты данных на указанный узел и показывает, сколько из них дошло до цели.

Использование команды ping:

* Открыть командную строку (Windows) или терминал (Mac/Linux);
* Ввести команду ***ping адрес\_сайта*** и нажать Enter;
* Результаты покажут количество отправленных и полученных пакетов, а также среднее время отклика. Сообщения о потере пакетов указывают на проблему.

Некоторые опции команды ping:

* ***-t*** — непрерывная отправка пакетов до прерывания (сочетание клавиш Ctrl+C);
* ***-c количество\_пакетов*** — отправка указанного количества пакетов;
* ***-i интервал*** — изменение интервала между отправкой пакетов (по умолчанию — 1 секунда).

Команда traceroute

Команда traceroute показывает путь, по которому проходят пакеты до указанного сервера или IP-адреса.

Использование команды traceroute:

* Открыть командную строку (Windows) или терминал (Mac/Linux);
* Ввести команду ***tracert адрес\_сайта*** (Windows) или ***traceroute адрес\_сайта*** (Mac/Linux);
* Результаты отобразят список промежуточных узлов, время отклика до каждого из них и IP-адреса.

Некоторые опции команды traceroute:

* ***-h максимальное\_количество\_переходов*** — указание максимального количества переходов;
* ***-n*** — исключение доменных имён из результатов.

Команда show commands

Команда show commands используется для диагностики сети, например, на устройствах Cisco.

Использование команды show:

* ***show interfaces*** — показывает статус и конфигурацию интерфейсов;
* ***show running-config*** — отображает текущую конфигурацию устройства;
* ***show version*** — показывает версию программного обеспечения и конфигурацию оборудования.

Чтобы просмотреть список доступных команд, нужно ввести ***show command?*** в командной строке.