?????????? ?????? ????????? ???? ?????????? «SDU UNIVERSITY»

СОДЕРЖАНИЕ

1. Архитектура и проектирование сети

1.1 Топология сети

1.2 Резервирование

1.3 Масштабируемость

1.4 Сегментация

2. Контроль доступа и безопасность

2.1 Аутентификация пользователей

2.2 Авторизация

2.3 Брандмауэры и системы IDS/IPS

2.4 Шифрование

2.5 Виртуальная частная сеть (VPN)

2.6 Обновления безопасности

3. Производительность сети и качество обслуживания (QoS)

3.1 Управление пропускной способностью

3.2 Приоритезация трафика

3.3 Мониторинг

4. Восстановление после сбоев и непрерывность бизнеса

4.1 Резервное копирование

4.2 Процедуры восстановления

4.3 Репликация данных

5. Соблюдение нормативных требований и юридические аспекты

5.1 Регулирование защиты данных

5.2 Отраслевые стандарты

5.3 Аудиторские следы

6. Обслуживание и поддержка

6.1 Плановое обслуживание

6.2 Поддержка поставщиков

6.3 Устранение неполадок

6.4 Документация

7. Обучение и осведомленность

7.1 Обучение пользователей

7.2 Обучение IT-специалистов

8. Реагирование на инциденты и отчетность

8.1 Управление инцидентами

8.2 Судебная экспертиза

8.3 Обзор после инцидента

9. Доступ к сети и удаленная работа

9.1 Контроль доступа для удаленной работы

9.2 Безопасность удаленных устройств

9.3 Управление мобильными устройствами (MDM)

11. Документация и отчетность по сети

11.1 Диаграммы сети

11.2 Управление изменениями

11.3 Отчеты по производительности

1. ??????????? ? ????????????? ????

1.1 ????????? ????

- Сеть должна быть построена с использованием эффективной топологии, которая подходит для масштабируемости и доступности.

- Предпочтительная топология — «звезда», если необходимо обеспечить централизованное управление и легкость в диагностике.
- Использование кольцевой топологии допустимо только при наличии механизмов для автоматического восстановления в случае отказа.
- Не допускается использование шинной топологии для крупных и критичных бизнес-приложений из-за рисков каскадных отказов.

1.2 ??????????????

- Все критичные компоненты сети (например, серверы, маршрутизаторы, коммутаторы) должны иметь резервные источники питания и каналы связи для обеспечения непрерывной работы.
- Для каждого ключевого сетевого узла должен быть предусмотрен резервный путь передачи данных, обеспечивающий автоматическое переключение в случае отказа основного канала.
- Регулярно проводить тесты восстановления работы сети с использованием резервных систем и каналов.
- Использование технологии отказоустойчивости на уровне программного обеспечения (например, протоколы HSRP, VRRP) обязательно для всех маршрутизаторов и шлюзов.

1.3 ???????????????

- Сеть должна быть спроектирована с расчетом на будущие расширения и увеличение нагрузки.
- Планирование пропускной способности должно учитывать потенциальный рост трафика в течение как минимум 3-5 лет.
- Все сетевые устройства должны поддерживать возможность расширения пропускной способности и добавления дополнительных портов без значительных изменений в архитектуре.
- Применение технологий виртуализации и SDN (Software-Defined Networking) для динамического увеличения пропускной способности и адаптации инфраструктуры к изменяющимся требованиям обязательно.

1.4 ??????????

- Сеть должна быть сегментирована с использованием VLAN для изоляции различных типов трафика и повышения безопасности.

- Каждому отделу или функциональной группе следует выделять отдельную VLAN для улучшения контроля доступа и минимизации рисков распространения угроз.
- Виртуальные сети для критичных данных должны быть полностью изолированы от остальных сегментов сети и защищены с использованием межсетевых экранов (firewalls) и средств контроля доступа.
- Ограничение маршрутизации между VLAN должно быть настроено с учетом принципа минимальных привилегий, чтобы предотвратить несанкционированный доступ к чувствительной информации.

2. ???????? ??????? ? ???????????

2.1 ?????????????? ??????????

- Все пользователи, включая сотрудников и сторонних участников, обязаны проходить многофакторную аутентификацию (MFA) для доступа к корпоративной сети.
- В случае использования паролей, они должны быть сложными, состоящими минимум из 12 символов, включая заглавные и строчные буквы, цифры и специальные символы.
- Использование однофакторной аутентификации (например, только пароля) запрещено для всех критичных систем и сервисов.
- Пользователи должны регулярно менять свои пароли, как минимум раз в 90 дней.
- Доступ к сети должен быть ограничен на основе ролей, с использованием строгих механизмов контроля, таких как Single Sign-On (SSO), для минимизации количества паролей.

2.2 ??????????

- Принцип наименьших привилегий должен быть применен ко всем пользователям и системам: доступ к данным и ресурсам предоставляется только на основе минимально необходимого уровня.
- Права доступа должны быть строго контролируемыми и пересматриваться не реже одного раза в год.
- Каждый пользователь должен иметь уникальные учетные записи для работы в системе. Коллективные учетные записи или общие пароли

запрещены.

- Доступ к критичным системам и данным (например, финансовая информация, персональные данные) должен быть ограничен только авторизованным пользователям с соответствующими правами.
- Все изменения в уровнях доступа должны фиксироваться и подлежать аудиту.

2.3 ??????????? ? ??????? IDS/IPS

- Все сетевые устройства, включая маршрутизаторы и серверы, должны быть защищены брандмауэрами, настроенными для блокировки несанкционированного доступа как с внешней, так и с внутренней стороны сети.
- Брандмауэры должны быть настроены с учетом предсказуемого трафика и потенциальных угроз, и их конфигурация должна быть регулярно проверяема и обновляема.
- В сети должны быть внедрены системы обнаружения и предотвращения вторжений (IDS/IPS), которые должны мониторить весь трафик в реальном времени и немедленно реагировать на подозрительную активность.
- Все инциденты, выявленные системой IDS/IPS, должны немедленно анализироваться и документироваться для дальнейшего расследования.

2.4 ??????????

- Все чувствительные данные, включая личные данные сотрудников и клиентов, должны быть зашифрованы как в покое, так и при передаче.
- Для шифрования данных должны использоваться современные и признанные алгоритмы, такие как AES-256 для хранения и TLS 1.2 или выше для передачи.
- Все каналы связи, в том числе внешние и удаленные соединения, должны использовать безопасные протоколы передачи данных, такие как HTTPS, SSH и другие стандарты шифрования.
- Логины и пароли, передаваемые через сеть, обязаны шифроваться с использованием протоколов, обеспечивающих высокий уровень защиты.

2.5 ??????????? ??????? ???? (VPN)

- Все удаленные пользователи, а также сотрудники, работающие из дома или в командировках, должны использовать VPN для подключения к

корпоративной сети.

- VPN должен поддерживать современные методы шифрования и обеспечения безопасности, включая использование протоколов IKEv2 или OpenVPN.
- Пользователи VPN должны быть аутентифицированы с использованием многофакторной аутентификации (MFA).
- Все сессии VPN должны быть журналируемыми, и доступ к журналам должен быть ограничен для обеспечения конфиденциальности и целостности данных.

2.6 ?????????? ????????????

- Все сетевые устройства и программное обеспечение должны регулярно получать обновления безопасности, которые должны быть внедрены в течение 72 часов с момента выпуска патча.
- Для критичных систем обновления должны быть протестированы в тестовой среде перед развертыванием в рабочей сети.
- Все обновления безопасности должны быть документированы и их внедрение должно сопровождаться проверкой на наличие уязвимостей после применения патча.
- Периодически проводите аудит безопасности с целью выявления устаревших систем и программного обеспечения, которые больше не поддерживаются или имеют известные уязвимости.

3. ???????????????? ???? ? ???????? ???????????? (QoS)

3.1 ?????????? ?????????? ????????????

- Пропускная способность сети должна быть спроектирована с учетом требований всех критичных приложений предприятия, таких как ERP-системы, базы данных и веб-сервисы.
- Сетевая инфраструктура должна обеспечивать достаточную пропускную способность с учетом текущих и прогнозируемых нагрузок на протяжении как минимум следующих 3 лет.
- Пропускная способность каналов связи должна быть достаточной для покрытия пиковых нагрузок, не создавая узких мест в работе сети.

- Для защиты от перегрузок и обеспечения бесперебойной работы бизнес-критичных приложений должна быть внедрена резервная пропускная способность.
- При необходимости пропускная способность должна быть динамически регулируемой с использованием технологий, таких как SD-WAN, чтобы обеспечить плавную работу бизнеса.

3.2 ????????????? ???????

- В сети должно быть реализовано управление качеством обслуживания (QoS), чтобы приоритизировать трафик критичных приложений и услуг.
- Все приложения, чувствительные к задержкам (например, VoIP, видеоконференции, системы мониторинга), должны быть выделены в приоритетные классы трафика.
- Протоколы QoS должны включать в себя управление задержками, джиттером и потерями пакетов, чтобы гарантировать стабильную работу приложений в реальном времени.
- Правила приоритизации должны быть настроены для различных типов трафика, включая голосовой и видеоданные, чтобы предотвратить их ухудшение при перегрузке сети.
- Необходимо использовать механизмы, такие как Weighted Fair Queuing (WFQ) или Differentiated Services (DiffServ), для оптимального распределения пропускной способности сети среди различных типов трафика.

3.3 ??????????

- Все компоненты сети должны быть под постоянным мониторингом с использованием специализированных инструментов для измерения производительности, доступности и стабильности сети.
- Рекомендуется внедрить систему мониторинга, которая отслеживает использование пропускной способности в реальном времени, чтобы своевременно выявлять и устранять узкие места.
- Все сетевые устройства и каналы связи должны регулярно проверяться на предмет их текущей загрузки и производительности.
- Для раннего обнаружения проблем с производительностью и доступностью сети должны быть настроены оповещения и уведомления,

чтобы минимизировать время отклика на инциденты.

- Системы мониторинга должны генерировать отчеты, которые используются для анализа производительности и планирования расширений сети.

4. ????????????? ????? ????? ? ????????????? ???????

4.1 ????????? ???????????

- Все критичные данные и конфигурации сетевых устройств должны регулярно резервироваться не реже одного раза в сутки.
- Процесс резервного копирования должен включать как данные, так и настройки всех сетевых устройств (маршрутизаторы, коммутаторы, серверы и т.д.).
- Резервные копии должны храниться в безопасных местах, обеспечивающих защиту от физического и логического доступа, а также от природных бедствий.
- Необходимо обеспечить наличие локальных и удаленных резервных копий. В идеале одна копия должна храниться в географически удаленном месте, чтобы предотвратить потерю данных в случае физической катастрофы на основном объекте.
- Резервные копии должны быть зашифрованы и защищены от несанкционированного доступа.
- Регулярно проверяйте целостность и актуальность резервных копий, чтобы гарантировать их работоспособность в случае необходимости восстановления.

4.2 ????????? ?????????????

- Все процессы восстановления после сбоев должны быть документированы и четко определены. Включите пошаговые инструкции для восстановления работы сети, начиная с восстановления критичных сервисов и заканчивая полным восстановлением всех систем.
- Процедуры восстановления должны быть протестированы хотя бы раз в квартал с реальными сценариями сбоев, чтобы убедиться, что все участники процесса знают свои обязанности и могут быстро восстановить сеть.

- В случае восстановления после катастрофы должен быть установлен приоритет для восстановления наиболее важных для бизнеса приложений и сервисов.
- Процесс восстановления должен включать в себя использование резервных копий конфигураций и данных, а также автоматизацию, где это возможно, для сокращения времени простоя.
- Определите и поддерживайте минимальное время восстановления (RTO) и допустимый уровень потери данных (RPO), чтобы гарантировать соблюдение требований бизнеса.

4.3 ?????????? ??????

- Все критичные данные компании должны быть реплицированы в географически распределенных местах для обеспечения высокой доступности и устойчивости к сбоям.
- Репликация данных должна быть настроена с использованием технологий, таких как синхронная и асинхронная репликация, в зависимости от критичности данных и уровня доступности, который требуется для бизнеса.
- Важно, чтобы репликация данных обеспечивала целостность и доступность информации в случае сбоя в основном центре обработки данных.
- Репликация должна покрывать как основные данные, так и конфигурации критичных систем (например, базы данных, виртуальные машины, конфигурации сетевых устройств).
- Регулярно проверяйте работоспособность процессов репликации, чтобы гарантировать, что данные доступны для восстановления в случае аварийной ситуации.

5. ?????????? ??????????? ?????????? ? ??????????? ???????

5.1 ????????????? ?????? ??????

- Соблюдайте все применимые законы и нормативные акты о защите данных, такие как GDPR, CCPA и другие, для всех данных, передаваемых, хранимых и обрабатываемых в сети.

- Все персональные данные должны быть зашифрованы как в покое, так и при передаче, чтобы минимизировать риск утечек данных.
- Обеспечьте соблюдение принципа минимизации данных, собирая только те данные, которые необходимы для выполнения бизнес-процессов.
- Регулярно проводите обучение сотрудников и проверку процессов обработки данных для гарантии соблюдения всех требований в области защиты данных.
- Внедрите процессы для быстрого реагирования на запросы о доступе к данным и их удалении в соответствии с требованиями законодательства.

5.2 ?????????? ?????????

- Следуйте признанным международным и отраслевым стандартам, таким как NIST, ISO 27001, для обеспечения безопасности сети и ее эксплуатации.
- Все сетевые процессы и системы должны быть спроектированы и проверены на соответствие актуальным стандартам безопасности, включая меры по защите от вторжений, контролю доступа и защите конфиденциальности.
- Регулярно обновляйте политики безопасности, чтобы они соответствовали изменениям в отраслевых стандартах и требованиям регулирования.
- Участие в независимых аудиторских проверках и сертификациях (например, ISO 27001) обязательно для всех критичных сетевых компонентов и процессов.

5.3 ??????????? ?????

- Ведите подробные журналы всех событий в сети, включая доступ пользователей, изменения конфигураций и системы, а также инциденты безопасности.
- Журналы доступа и изменений должны содержать информацию о времени, пользователе, IP-адресе и деталях действий.
- Все журналы должны быть защищены от несанкционированного доступа и храниться в течение как минимум 12 месяцев, чтобы обеспечить соответствие требованиям аудита.
- Доступ к журналам должен быть ограничен только уполномоченным персоналом, а доступ к ним должен быть строго контролируемым и

зафиксированным в журнале.

6. ??????????? ? ?????????

6.1 ???????? ????????????

- Разработайте и поддерживайте регулярный график технического обслуживания для обновления сетевых устройств, программного обеспечения и систем безопасности.
- Проводите плановые проверки и обновления на регулярной основе, чтобы исключить риски от устаревших компонентов или уязвимостей.
- Все обновления и установки должны быть протестированы на тестовой среде перед применением в рабочей сети.
- Составьте и утвердите план технического обслуживания для каждого ключевого компонента сети, включая сроки обслуживания и процедуры.

6.2 ????????? ???????????

- Обеспечьте наличие действующих контрактов с поставщиками оборудования и программного обеспечения, обеспечивающих актуальную поддержку, обслуживание и гарантийные услуги.
- Все контракты с поставщиками должны включать условия по срокам реакции на инциденты, доступности технической поддержки и условиях обновления программного обеспечения.
- Поставщики должны регулярно предоставлять отчеты о состоянии системы, включая уязвимости и планируемые обновления безопасности.
- Убедитесь, что все договоренности с поставщиками четко прописаны в контрактах и регулярно пересматриваются.

6.3 ?????????? ?????????

- Разработайте и внедрите процесс диагностики и устранения проблем с сетью, включающий четкие шаги по выявлению и устранению неисправностей.
- Используйте диагностические инструменты и мониторинг для своевременного выявления и решения проблем с производительностью, доступностью и безопасностью сети.
- Установите механизмы эскалации, чтобы при необходимости привлекать специалистов для более сложных проблем.

- Каждая неисправность должна быть документирована, и должна быть проведена последующая оценка, чтобы избежать повторения аналогичных инцидентов.
- Регулярно проводите тренировки и тесты для персонала, чтобы они могли оперативно устранять неполадки в случае сбоев.

6.4 ???????????

- Поддерживайте полную и актуальную документацию на все сетевые устройства, конфигурации и процессы устранения неполадок.
- Документация должна включать схемы сети, описание используемых технологий и протоколов, а также инструкции для обслуживания и ремонта оборудования.
- Обновление документации должно осуществляться сразу после любых изменений в сети или оборудовании, чтобы она всегда оставалась актуальной.
- Документация должна быть доступна только уполномоченному персоналу и защищена от несанкционированного доступа.

7. ???????? ? ??????????????

7.1 ???????? ?????????????

- Все сотрудники должны проходить регулярные курсы по безопасности, включая обучение лучшим практикам защиты данных, предотвращению фишинга и безопасному использованию сетевых ресурсов.
- Вся информация и материалы по безопасности должны быть понятными и доступными для сотрудников разных уровней.
- Обучение должно включать регулярные тренировки по действиям в случае инцидентов безопасности, таких как фишинг или утечка данных.
- Сотрудники должны проходить обновленное обучение по безопасности хотя бы раз в год.
- Все работники должны подписывать соглашения о конфиденциальности и подтверждать, что они ознакомлены с внутренними политиками безопасности.

7.2 ???????? IT-????????????

- IT-специалисты должны проходить специализированное обучение по управлению сетью, устранению неполадок и соблюдению протоколов

безопасности.

- Обучение должно быть регулярным и включать как теоретические, так и практические занятия, направленные на развитие технических навыков.
- Все специалисты по безопасности должны иметь сертификации в области защиты информации, такие как CISSP, CISM или другие признанные в отрасли.
- IT-отдел должен быть обучен в реагировании на инциденты безопасности, включая соблюдение политики защиты данных и минимизацию воздействия на инфраструктуру сети.
- Все технические специалисты должны быть ознакомлены с текущими уязвимостями и обновлениями безопасности для поддержания уровня квалификации.

8. ???????????? ?? ????????? ? ??????????

8.1 ?????????? ???????????

- Должен быть четко определен процесс сообщения, обработки и эскалации инцидентов в сети, включая коммуникацию с пострадавшими сторонами.
- Все инциденты безопасности должны быть зарегистрированы и классифицированы по степени критичности, с соответствующими временными рамками для разрешения.
- Все инциденты должны иметь зафиксированные меры реагирования, включая шаги по локализации, исправлению и предотвращению повторных атак.
- Процесс обработки инцидентов должен быть автоматизирован, чтобы ускорить выявление и решение проблем.
- В случае серьезных инцидентов должна быть немедленно сформирована группа для управления кризисной ситуацией.

8.2 ???????? ??????????

- В случае нарушения безопасности должны быть использованы инструменты для сбора и анализа данных, чтобы определить причины инцидента и оценить его последствия.

- Все данные, связанные с инцидентом, должны быть сохранены в соответствии с нормативами и требованиями безопасности для дальнейшего анализа.
- Собранные данные должны быть защищены от несанкционированного доступа и использованы только для расследования инцидента.
- В случае необходимости, данные из инцидентов могут быть использованы для судебных разбирательств, в том числе в соответствии с требованиями законодательства о защите данных.
- Процесс судебной экспертизы должен быть поддержан инструментами, которые обеспечивают точность и полноту расследования.

8.3 ????? ????? ?????????

- После каждого инцидента должно быть проведено детальное расследование для выявления слабых мест в системе безопасности и принятия мер по улучшению защитных механизмов.
- Все инциденты должны быть проанализированы с целью выявления корневых причин и предотвращения их повторения.
- Рекомендации по улучшению защиты должны быть разработаны на основе опыта, полученного в ходе инцидента, и внедрены в процессы безопасности.
- Результаты обзора после инцидента должны быть задокументированы и доведены до сведения всех заинтересованных сторон.
- Необходимо провести дополнительные тренировки для персонала, чтобы усилить безопасность и минимизировать вероятность будущих инцидентов.

9. ?????? ? ???? ? ????????? ??????

9.1 ???????? ??????? ??? ????????? ??????

- Все сотрудники, работающие удаленно, должны использовать безопасные методы подключения к сети, такие как VPN или Single Sign-On (SSO), для обеспечения защищенного доступа.
- Доступ к корпоративным ресурсам должен быть ограничен только теми пользователями, которые имеют необходимое разрешение для работы с данными.

- Все удаленные соединения должны быть зашифрованы, а аутентификация пользователей — многофакторной, чтобы минимизировать риски.
- Доступ к сети должен быть организован с учетом наименьших привилегий, ограничивая доступ к необходимым только приложениям и данным.
- Периодически проводите ревизию прав доступа сотрудников, работающих удаленно, чтобы поддерживать безопасность сети.

9.2 ??????????? ????????? ?????????

- Все удаленные устройства, подключающиеся к корпоративной сети, должны быть защищены средствами безопасности, такими как антивирусные программы и шифрование дисков.
- Устройства должны быть настроены таким образом, чтобы автоматически устанавливать обновления безопасности и проверки на наличие угроз.
- Удаленные устройства должны быть зарегистрированы и мониториться для своевременного выявления угроз или нарушений безопасности.
- Использование личных устройств для работы с корпоративными данными должно быть строго контролируемым и обеспечиваться политиками безопасности.
- Все устройства, используемые для удаленной работы, должны иметь настройки, предотвращающие утечку корпоративной информации.

9.3 ?????????? ?????????? ???????????? (MDM)

- Для всех мобильных устройств, подключающихся к корпоративной сети, должно быть внедрено управление мобильными устройствами (MDM).
- MDM должна обеспечивать возможность централизованного контроля за устройствами, включая мониторинг, управление приложениями и установку обновлений безопасности.
- Все мобильные устройства должны быть защищены от несанкционированного доступа с помощью PIN-кодов, паролей или биометрической аутентификации.
- В случае утери или кражи мобильного устройства должна быть возможность удаленно заблокировать устройство или стереть все данные.

- Политики MDM должны включать ограничения на установку сторонних приложений и передачу данных между устройствами и корпоративной сетью.

11. ???????????? ? ?????????? ?? ????

11.1 ????????? ????

- Все архитектурные схемы сети, включая конфигурации и соединения, должны быть актуальными и регулярно обновляемыми.
- Диаграммы сети должны быть четкими, понятными и отражать все компоненты сети, включая устройства, маршруты, сегменты и точки подключения.
- Вся информация о компонентах сети должна быть интегрирована в документацию с подробными сведениями о настройках, IP-адресах и физической топологии.
- Диаграммы сети должны быть доступны только авторизованным пользователям для предотвращения утечек информации о конфиденциальной инфраструктуре.

11.2 ?????????? ???????????

- Все изменения в сети, включая обновления оборудования, программного обеспечения и конфигураций, должны быть задокументированы и отслеживаемы через систему управления изменениями.
- Каждый процесс изменения должен быть одобрен заранее и сопровождаться детализированным планом действий и оценкой возможных рисков.
- Для каждого изменения должны быть задокументированы соответствующие тесты, проверки и процедуры отката, чтобы гарантировать минимизацию возможных нарушений в сети.
- Все изменения должны быть рассмотрены с точки зрения безопасности и соответствовать внутренним политикам компании.
- Все изменения должны быть задокументированы в реальном времени для обеспечения точности данных и соблюдения аудита.

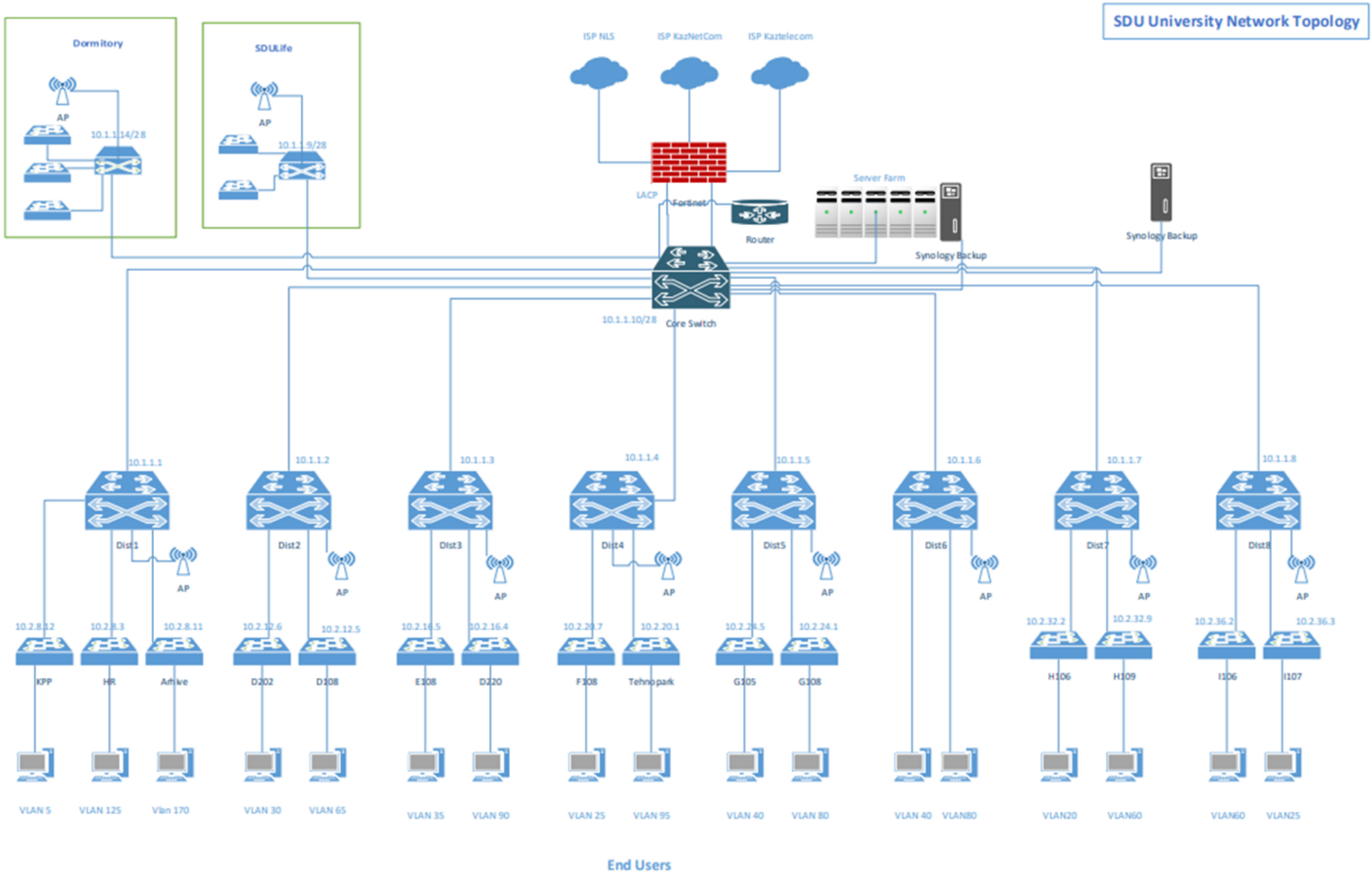
11.3 ?????? ?? ??????????????????

- Регулярно предоставляйте отчеты о производительности сети руководству, с указанием ключевых показателей, таких как пропускная

способность, задержки и доступность сервисов.

- В отчетах должны быть описаны узкие места, проблемы с производительностью и предложены меры для их устранения.
- Отчеты должны включать статистику по использованию сети, включая топологию трафика и потребление ресурсов.
- Отчеты должны быть представлены в формате, который легко анализируется для принятия управленческих решений по улучшению производительности сети.
- Руководству должны предоставляться рекомендации по оптимизации и планированию будущих изменений для поддержания высокого уровня доступности и производительности сети.

?????????? 1


SDU University Network Topology
Dormitory
AP
10.1.1.14/28
SDULife
AP
10.1.1.9/28
ISP NLS
ISP KazNetCom
ISP Kaztelecom
LACP
FortiGate
Router
Server Farm
Synology Backup
Synology Backup
10.1.1.10/28
Core Switch
10.1.1.1
Dist1
AP
10.2.8.12
10.2.8.3
10.2.8.11
KPP
HR
Archive
VLAN 5
VLAN 125
Vlan 170
10.1.1.2
Dist2
AP
10.2.12.6
10.2.12.5
D202
D108
VLAN 30
VLAN 65
10.1.1.3
Dist3
AP
10.2.16.5
10.2.16.4
E108
D220
VLAN 35
VLAN 90
10.1.1.4
Dist4
AP
10.2.20.7
10.2.20.1
F108
Tehnopark
VLAN 25
VLAN 95
10.1.1.5
Dist5
AP
10.2.24.5
10.2.24.1
G105
G108
VLAN 40
VLAN 80
10.1.1.6
Dist6
AP
VLAN 40
VLAN80
10.1.1.7
Dist7
AP
10.2.32.2
10.2.32.9
H106
H109
VLAN20
VLAN60
10.1.1.8
Dist8
AP
10.2.36.2
10.2.36.3
I106
I107
VLAN60
VLAN25
End Users

Revision #1
Created 2026-01-23 10:16:52 UTC by Ibrahim Tuncer
Updated 2026-01-23 10:24:14 UTC by Ibrahim Tuncer