Добрый день, уважаемые эксперты!  
Сегодня я представлю результаты своей работы по выполнению конкурсного задания. Постараюсь кратко осветить ключевые этапы и решения.

**1. Сетевая инфраструктура**

1. **Туннелирование и безопасность:**
   * Настроены GRE-туннели между AR, VYOS и PFSENSE с защитой IPSec (IKEv2 + PSK).
   * Для динамической маршрутизации использован OSPF внутри туннелей, что обеспечило связность между офисами и ЦОД.
   * Реализован BGP между Leaf/Spine коммутаторами для EVPN (адрес-семейство L2VPN).
2. **EVPN/VxLAN в ЦОД:**
   * Настроены L2VNI (VLAN 100-300) и L3VNI для меж-VLAN маршрутизации в рамках VRF.
   * Использован Anycast Gateway (SVI с одинаковым IP на Leaf) для распределенных шлюзов.
   * Проверена корректность анонсов маршрутов Type-2 (MAC/IP) и Type-5 (префиксы) через BGP.
3. **Агрегация и отказоустойчивость:**
   * Созданы LACP-каналы между SW1-SW2-SW3 с активным режимом на SW1.
   * Настроены транки только для используемых VLAN (Native VLAN для управления исключен из транков).
4. **Underlay/Overlay маршрутизация:**
   * Underlay: OSPF с аутентификацией (пароль: P@ssw0rd) в глобальной таблице маршрутизации.
   * Overlay: iBGP между Leaf и Spine (AS 65101), Spine как Route Reflector.
5. **Доступ в интернет:**
   * NAT настроен для зон INFRA/MGMT через провайдера MOONET (основной) и GIGAFON (резервный).
   * iBGP между маршрутизаторами через VLAN 999 для балансировки трафика.

**2. Безопасность и аутентификация**

1. **Доступ к сетевым устройствам:**
   * SSH с RADIUS-аутентификацией через ALD Pro (DC-A). Локальный пользователь *atom* с правами sudo.
   * На AR настроен резервный вход через локальную учетную запись *super* (пароль: super).
2. **Интеграция ALD Pro:**
   * Домены office.atom25.local и branch.atom25.local с двусторонним доверием.
   * Миграция пользователей из Windows-домена в ALD Pro с сохранением групп (core-web-admins, core-wd-admins).
3. **Keycloak и SSO:**
   * Реалм ATOM25 с синхронизацией пользователей через LDAP (режим Read-Only).
   * Настройка токенов: срок действия — 2 минуты, одноразовый Refresh Token.
   * Интеграция с корпоративным приложением через OpenID Connect.
4. **Центр сертификации (Windows):**
   * Развернут корневой ЦС на COD-WEB (WinAtom-RootCA) с публикацией CRL/AIA.
   * Шаблоны сертификатов: Web Site (для COD-WEB) и Web Admin Access (для core-web-admins).

**3. Сервисы Linux**

1. **NFS и синхронизация:**
   * Перемещаемые профили пользователей на SRV-A (NFSv4) с синхронизацией между офисами через rsync (интервал ≤30 сек).
   * Общие каталоги (Share, Docs, Secret) с ACL:
     + *Secret* доступен только для core-wd-admins через маскировку в .hidden.
2. **Почтовый сервер:**
   * Отправка писем между aarozhkov (CLI-A) и emsmirnova (CLI-B) через защищенное соединение (TLS).
   * Авторизация через Kerberos (логин в формате [username@office.atom25.local](https://mailto:username@office.atom25.local/)).
3. **Прокси-сервер Squid:**
   * Ограничение доступа к site2.atom25.ru для филиала.
   * Авторизация на site1.atom25.ru через локальную базу (пользователи ivan/aleksey).
   * Ограничение скорости для .mp4/.png (10 Б/с) для пользователя aleksey.
4. **CI/CD и Docker:**
   * GitFlic с пайплайном для сборки образов (backend/frontend) и деплоя на CLOUD-PROD.
   * Автоматические тесты: pycodestyle и pytest для кода unittest.py.

**4. Windows-инфраструктура**

1. **Active Directory:**
   * Создание сайта Branch с репликацией каждые 15 минут.
   * Настройка LAPS для управления паролями локального администратора *winadmin*.
2. **Файловые службы:**
   * RAID-зеркало на COD-FS с квотами (300 МБ/пользователь) и аудитом удаления файлов.
   * DFS Namespace (AtomDFS) с каталогами Exchange-Folder и Shared-Resources.
3. **Групповые политики (GPO):**
   * Автоматическое подключение сетевого диска S: для доменных пользователей.
   * Блокировка стартового экрана Edge и установка фонового изображения для core-wd-admins.
4. **RDS и ADFS:**
   * Публикация Putty и MS Edge через портал rds.atom25.local.
   * Аутентификация через ADFS с возможностью смены пароля.

**5. Мониторинг и логирование**

1. **Zabbix:**
   * Мониторинг AR, VYOS, PFSENSE через SNMP (графики ICMP response time).
   * Агенты на серверах с защитой PSK. Дашборды: Network Devices (доступность) и Servers (CPU/RAM).
2. **Сбор логов:**
   * Централизованное хранение на CLOUD-MON (syslog, bash-history) с ротацией (1 МБ → сжатие, 2 версии).
   * Веб-доступ к логам через HTTPS (nginx с редиректом на 443 порт).
3. **Репозитории и пакеты:**
   * Корпоративный deb-репозиторий (repo.atom25.local) с подписью GPG (RSA 4096).
   * Пакет atom25-config для автоматизации установки Zabbix Agent и настройки SSH.

**6. Проблемы и их решение**

* **EVPN/VxLAN:** Возникли сложности с анонсом маршрутов Type-5. Решено через проверку BGP-соседства и настройку Route-Target.
* **Интеграция Keycloak и ALD Pro:** Ошибки синхронизации групп. Исправлено через корректное указание атрибутов в LDAP-маппинге.
* **NAT в PFSENSE:** Не работал резервный канал. Добавлены правила Firewall для мониторинга состояния линка.