**🔥 Полное руководство по настройке корпоративной IT-инфраструктуры**

**⏳ Временной лимит: 6 часов**

**🛠️ Что будем делать?**

* Разворачивать виртуальные машины с Astra Linux, MikroTik и pfSense
* Настраивать сеть, DHCP, NAT, VPN, Firewall
* Включать контроль доступа и мониторинг безопасности
* Использовать отечественные решения (Astra, ALD, Eltex, CyberProtect)

**📌 Часть 1: Разворачивание виртуальной инфраструктуры (1 час)**

**🖥️ 1.1. Подготовка оборудования**

Перед настройкой нужно убедиться, что у тебя есть:  
✅ Компьютер / сервер с достаточной мощностью (8 CPU, 16GB RAM)  
✅ Установленный **KVM/QEMU**, **VMware ESXi** или **VirtualBox**  
✅ ISO-образы для установки операционных систем

**📂 1.2. Скачивание образов**

**MikroTik CHR (Cloud Hosted Router)**  
🔗 [Скачать с официального сайта](https://mikrotik.com/download)  
Выбираем: **CHR RAW Disk Image**

**Astra Linux (FW1, C1, C2)**  
🔗 [Скачать Astra Linux](https://astralinux.ru/download/)  
Выбираем: **Astra Linux Common Edition / Special Edition**

**pfSense (FW2, IDS/IPS)**  
🔗 [Скачать pfSense](https://www.pfsense.org/download/)  
Выбираем: **ISO Installer**

**🛠️ 1.3. Создание виртуальных машин**

**KVM (QEMU)**

1. Создаем диск для MikroTik CHR:
2. qemu-img create -f qcow2 mikrotik-chr.qcow2 512M
3. Запускаем установку MikroTik:
4. qemu-system-x86\_64 -hda mikrotik-chr.qcow2 -m 256 -enable-kvm -net nic -net user

**VMware / VirtualBox**

1. Создаем ВМ
2. Указываем **CPU: 2, RAM: 2GB, HDD: 10GB**
3. Подключаем скачанный ISO
4. Запускаем установку

**📌 Часть 2: Настройка сети (1.5 часа)**

**🌐 2.1. Настройка MikroTik (Маршрутизация и DHCP)**

**🔹 2.1.1. Настройка базового IP**

Заходим в MikroTik:

1. /ip address add address=192.168.1.1/24 interface=ether1

**Проверка:**

1. /ip address print

Если видим 192.168.1.1/24 — всё ок.

**🔹 2.1.2. Настройка DHCP**

1. Создаем пул адресов:
2. /ip pool add name=dhcp-pool ranges=192.168.1.10-192.168.1.200
3. Настраиваем DHCP-сервер:
4. /ip dhcp-server add name=dhcp1 interface=ether1 address-pool=dhcp-pool disabled=no
5. Указываем настройки сети:
6. /ip dhcp-server network add address=192.168.1.0/24 gateway=192.168.1.1 dns-server=8.8.8.8

**Проверка:**

1. /ip dhcp-server lease print

**🔹 2.1.3. Настройка NAT**

1. /ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

**Проверка доступа в интернет:**

1. ping 8.8.8.8

Если пингуется – отлично, NAT работает.

**🛡️ 2.2. Настройка Firewall (pfSense)**

1. Заходим в Web GUI **(**[**https://192.168.1.2:443**](https://192.168.1.2/)**)**
2. Переходим в **Firewall → Rules → WAN**
3. Нажимаем **Add Rule**
4. **Protocol:** TCP
5. **Destination Port:** 22 (SSH) / 443 (Web)
6. **Action:** Pass
7. **Apply Changes**

**📌 Часть 3: Настройка VPN (1.5 часа)**

**🔑 3.1. OpenVPN на MikroTik**

1. Включаем сервер:
2. /interface ovpn-server server set enabled=yes certificate=server-cert require-client-certificate=yes
3. Создаем пользователя:
4. /ppp secret add name=vpn-user password=StrongPass service=ovpn
5. Клиентская настройка (на рабочей станции):
6. /interface ovpn-client add connect-to=192.168.1.1 user=vpn-user password=StrongPass disabled=no
7. Проверяем подключение:
8. /interface ovpn-server print

**📌 Часть 4: Мониторинг и безопасность (1.5 часа)**

**🚨 4.1. IDS (Intrusion Detection System)**

**🛠️ 4.1.1. Установка Suricata (на Astra Linux)**

1. apt install suricata

**📜 4.1.2. Добавляем правило обнаружения атак**

1. echo "alert icmp any any -> any any (msg:'ICMP Packet Detected'; sid:1000001;)" >> /etc/suricata/rules/local.rules

**🔄 4.1.3. Перезапускаем IDS**

1. systemctl restart suricata

**📌 Часть 5: Финальная настройка и сдача (1 час)**

**📑 5.1. Создание документации**

**Обязательно включить в отчет:** ✅ Схему сети  
✅ IP-адреса и настройки сервисов  
✅ Конфигурацию DHCP, NAT, VPN  
✅ Скриншоты интерфейсов

**📂 5.2. Создание резервных копий**

**MikroTik:**

1. /export file=backup

**KVM/QEMU:**

1. virsh snapshot-create-as FW1 "Before Config" --description "Initial state"

**VMware:**

1. VM → Snapshot → Take Snapshot

**🚀 5.3. Финальная проверка перед сдачей**

✅ Интернет работает  
✅ Раздаются IP через DHCP  
✅ VPN подключается  
✅ IDS обнаруживает атаки  
✅ Отчет составлен