Сервисы по обеспечению безопасности дистанционного обучения

Александр Бекетов

Руководитель
направления ИБ СЗФО
a.bek@softline.com

Cloud | Security | Big Data | Mobility

softline®

Agenda

- Студенты и преподаватели на удаленке
- Защита учебных ресурсов
- Экзамены в новой реальности

Удаленный пользователь

Выделенное удаленное место (ноутбук)

Домашний компьютер подключенный к учебным ресурсам

Гибрид первых двух

Подключение к ресурсам УЗ с личного устройства

Технологии

- WiFi
- VPN
- RDP
- VDI
- Virtual App

Проблемы

- Старые версии ОС
- Отсутствие обновлений
- Пиратское ПО
- Антивирус?
- Расширения для браузеров

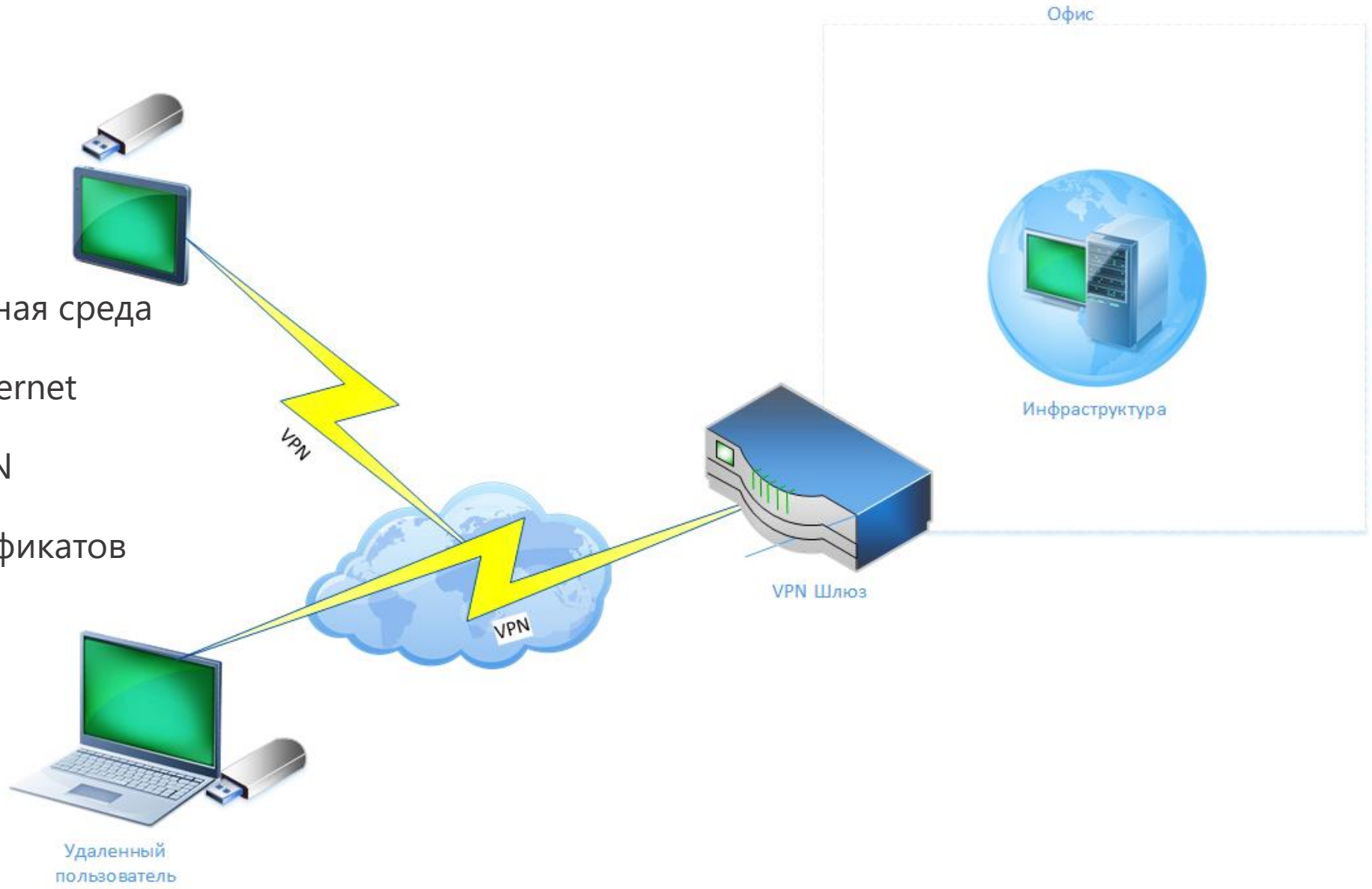
Гибрид

Полностью изолированная среда

Работа только через Ethernet

Работа только через VPN

Контроль и отзыв сертификатов



Защита ресурсов учебных заведений

Сканер безопасности

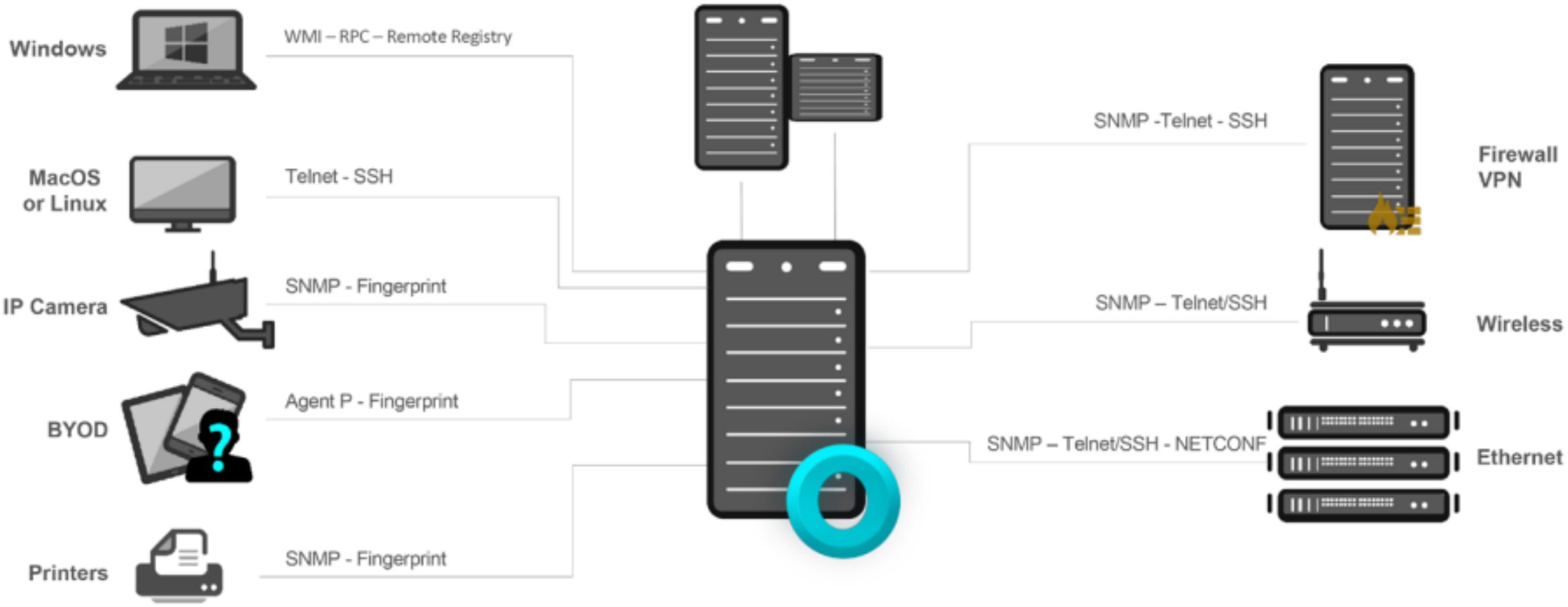
Network Access Control

Honeypot

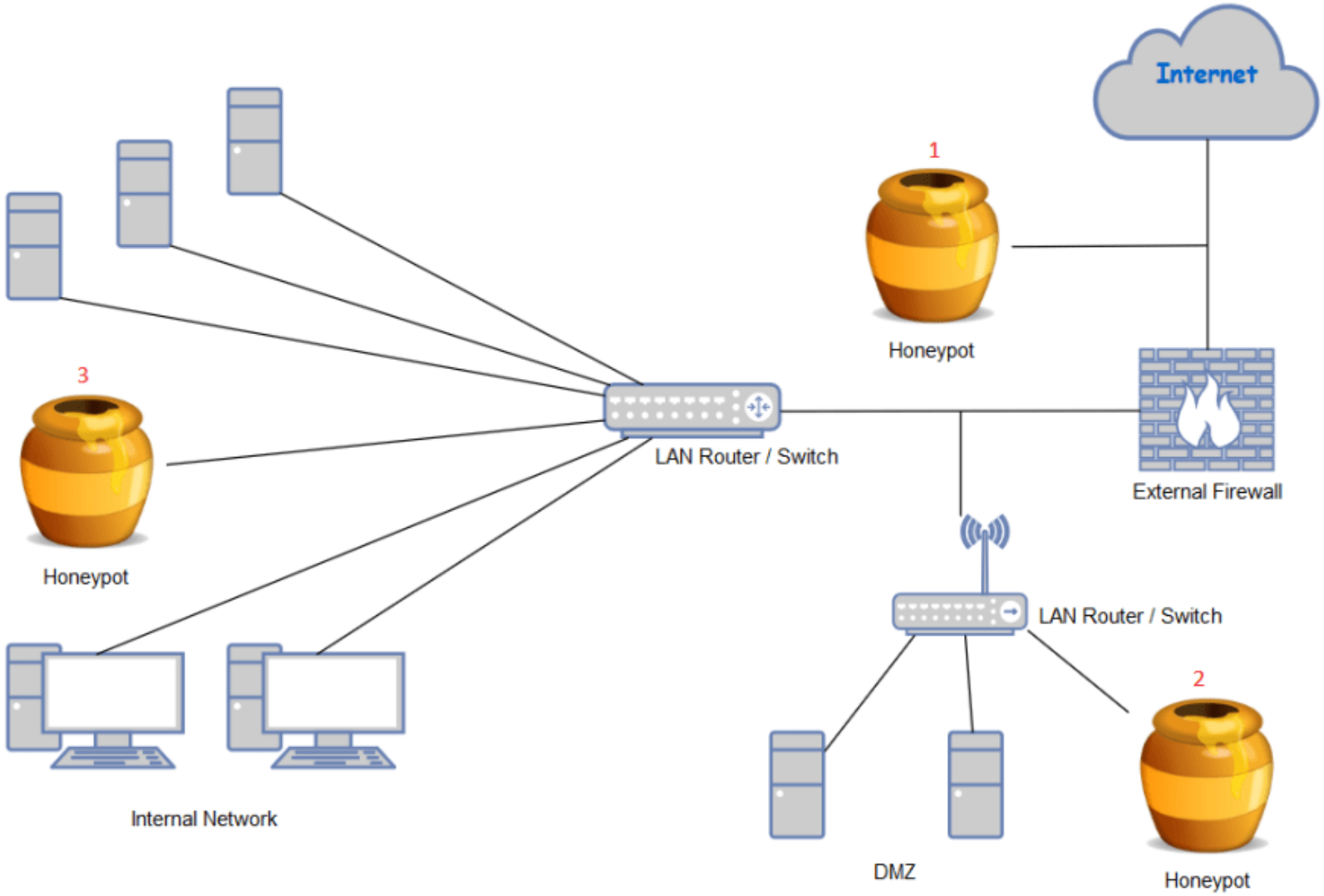
Моделирование атак

Повышение осведомленности персонала

NAC


Windows
WMI – RPC – Remote Registry
MacOS or Linux
Telnet - SSH
IP Camera
SNMP - Fingerprint
BYOD
Agent P - Fingerprint
Printers
SNMP - Fingerprint
SNMP -Telnet - SSH
Firewall VPN
SNMP – Telnet/SSH
Wireless
SNMP – Telnet/SSH - NETCONF
Ethernet

Honeypots

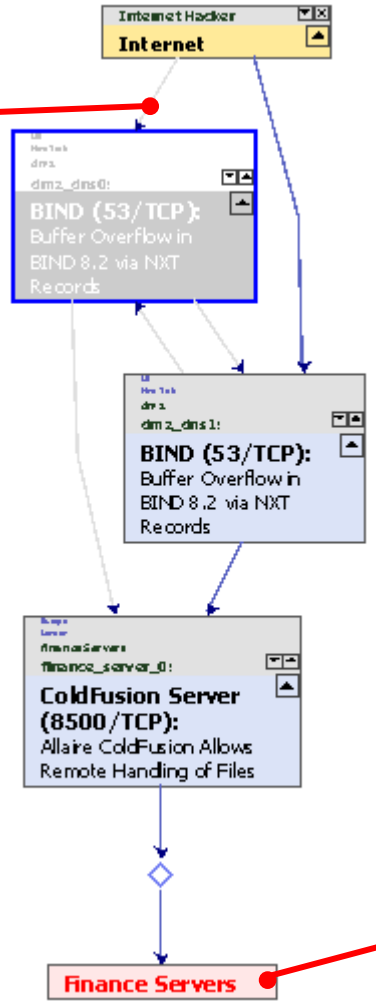

Internet
1
Honeypot
3
Honeypot
LAN Router / Switch
External Firewall
LAN Router / Switch
2
Honeypot
Internal Network
DMZ

Моделирование атак

Маршрут доступа

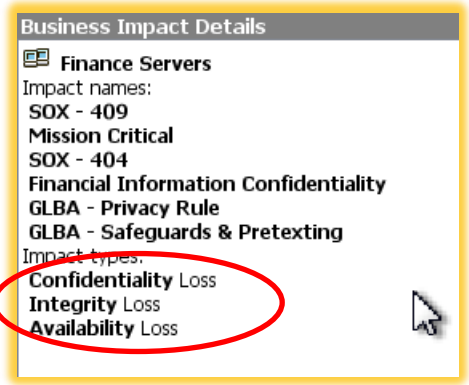
From **Internet (cloud)**
To **dmz_dns0 (BIND (53/TCP))**
There is a single route:

0. Internet (cloud)
   source IP range(s)
   0.0.0.0-9.255.255.255, 11.0.0.0-16.0.0.0, 16.0.0.2-172.15.255.255, ...
   source service(s): 1-65535/TCP
   destination IP range(s):
   192.170.33.32-192.170.33.32
   destination service(s): 53/TCP
1. main FW (16.0.0.1)
   Inbound access rule(s):
   2 (ACCESS) - Allow
   Routing rule(s):
   192.170.33.32 via interface 'int2809' (19, C)
2. prod FW (192.170.1.98)
   Inbound access rule(s):
   2 (ACCESS) - Allow
   Routing rule(s):
   192.170.33.32 via interface 'netIterface2088' (20)
3. dmz_dns0 (192.170.33.32)
   destination service(s): 53/TCP



Вероятный вектор атаки состоящий из нескольких шагов и пересекающий несколько сетевых зон

Влияние на бизнес



Повышение осведомленности

- Тренинги
- Памятки
  - Особенности удаленной работы:
  - Обработка персональных данных:
  - Ведение электронной переписки:
  - Защита от социальной инженерии.
- Фишинговые рассылки

Экзамены в новой реальности

Минимальные требования

CPU: 64-bit Dual Core (2.2 GHz per core)

RAM: 4 GB / 8 GB (Recommended)

Display resolution: 1024×768

HDD: Minimum 20GB available space

Устройства: внешняя или внутренняя веб-камера. Качество камеры должно обеспечить качественную передачу данных удостоверения личности.

Требования

Minimum required software for your host OS:

Operating system:

Windows 8.1 x64 / OSX Yosemite / MacOS

Virtualization Software:

VMware Player (Latest version), VMware Workstation 8.0, VMware Fusion 7.0

Browser:

Google Chrome 57.0

Internet:

Minimum 5mbps Download/ 1mbps Upload speeds

Stable connection that does not drop

Google Chrome Extension: Janus WebRTC Screensharing

Требования перед экзаменом

Экзаменатор попросит вас подтвердить, что вы ознакомлены с техническими требованиями, предъявляемым к экзамену.

Ваша личность будет подтверждена с помощью действительного государственного удостоверения личности, предъявленного в веб-камеру.

Вам будет предложено показать комнату с помощью веб-камеры.

Экзаменатор попросит вас поделиться всеми вашими экранами и отобразить все запущенные программы.

После подключения к экзаменационной VPN, экзаменатор проверит, что вы подключены только к экзаменационной VPN, и попросит вас запустить сценарий troubleshooting.sh, который включен в пакет VPN подключения.


GO GLOBAL
GO CLOUD
GO INNOVATIVE