员工侧安全

一站式解决方案最佳实践

止介(Feei)

FeeiCN

- 白帽子，Cobra、GSIL作者
- 专注漏洞自动化发现与防御
- 美丽联合集团 网络信息安全总监

美丽联合集团网络信息安全架构（2018 by Feei）

缺陷 | 深入中 | 建设中 | 未涉及

主动漏洞与情报发现

- 情报获取 Dylan
- 人工渗透测试 WhaleShark
- 测试团队 Test
- 漏洞靶场 IVTE
- 黑盒应用漏洞扫描器 Eagle
- 白盒代码审计系统 Cobra

被动漏洞与情报发现

- 安全应急响应中心 SRC
- 安全需求平台 Aone

安全运营

响应小组

- 安全技术评估组
- 安全理事会
- 各部门安全接口人

安全规范制定及落地推进

- 安全编码规范
- 框架/版本规范
- ACL策略/安全测试/应用上线/配置规范等

安全应急响应中心 SRC

培训（Train）

- 新人入职安全培训
- 业务开发安全培训

社交媒体（Media）

- 微博
- 微信公众号

- 安全风险评估
- 漏洞整改推进
- 漏洞管理平台 Hades
- 安全规范制定及落地推进
- 漏洞修复方案 Docs/Vul
- 安全规范法律、政策合规 网络安全法、GDPR、等级保护、安全认证
- 外部关系维护
- 内外部会议分享、交流
- 安全意识提升

Web（PC/H5）

- HTTP Only
- 滑块验证码
- 设备指纹
- 图形验证码

App（Android/iOS/小程序）

- 安全SDK
- 安全控件
- 加固 防逆向、防篡改 防调试、防窃取
- 设备指纹
- 图形/滑块验证码

HTTPS

网络（Network）

- DDoS 大禹
- 入侵检测系统 IDS
- Web/App应用网关防火墙 YMG
- 蜜罐系统 Honeypot
- 反爬虫 Anti-Spider

应用（Application）

- 应用运行间防护 RASP
- 漏洞修复组件 Begis

数据（Data）

- 数据资产 CMDB
- 数据防泄漏
- 数据查询平台 MDB
- 数据中间层 Raptor

主机（Server）

- 文件和命令监控 Afocus
- 安全基线和安全规范 Weapon&Claw
- ACL

- 流量代理 Proxy
- 堡垒机 Turtle

内部（Inner）

- 上网行为 Sonfor
- 统一登陆 Login
- 统一权限 Auth
- 统一审计 Audit

终端（End）

- 入网管控
- 统一免密鉴权
- 终端安全

Staff Endpoint Security

- Wi-Fi Attack
- VPN
- Username&Password
- Malware/Vulnerability
- LockScreen
- Security Config

Wi-Fi Attack

WiFi万能钥匙

AIRCRACK-NG

Social Engineering

VPN/Username&Password

Vulnerability&Malware

- CVE-2017-8768 SourceTree RCE <=2.5c
- JetBrains All IDES RCE&LFD <=2016.1
- XcodeGhost malware
- Sparkle Updater(iTerm/SequelPro/Tunnelblick) MITM&RCE

LockScreen


安全部all
下午请大家喝下午茶!
(1928)--1536129380020
快，拜见大佬
(1929)--1536129422898


安全部all
@天山，你为啥请我们喝下午茶啊?
(1930)--1536130361284
(1931)--1536130380178
谁搞的？？？
(1932)--1536130498212

Security Resolution

Zero Trust

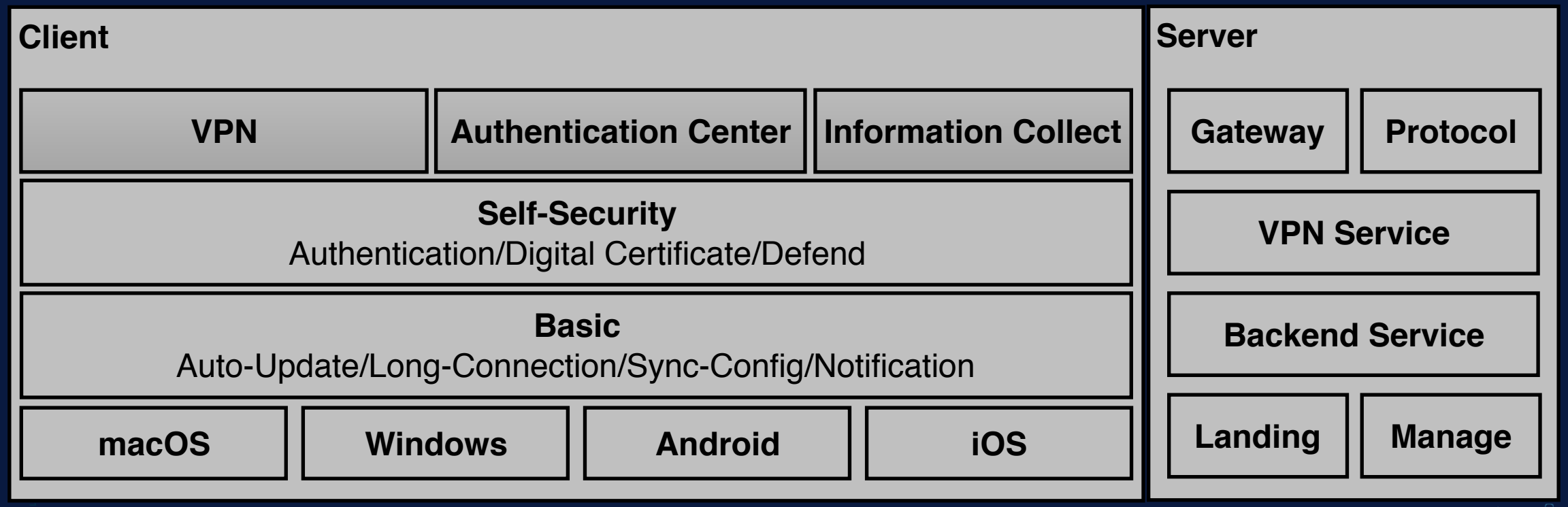
- No INTRANET
- No PASSWORD
- ANYTHING NEED AUTH
- AUTH BY USER+DEVICE
- TRAFIC AND AUDIT

Security Resolution

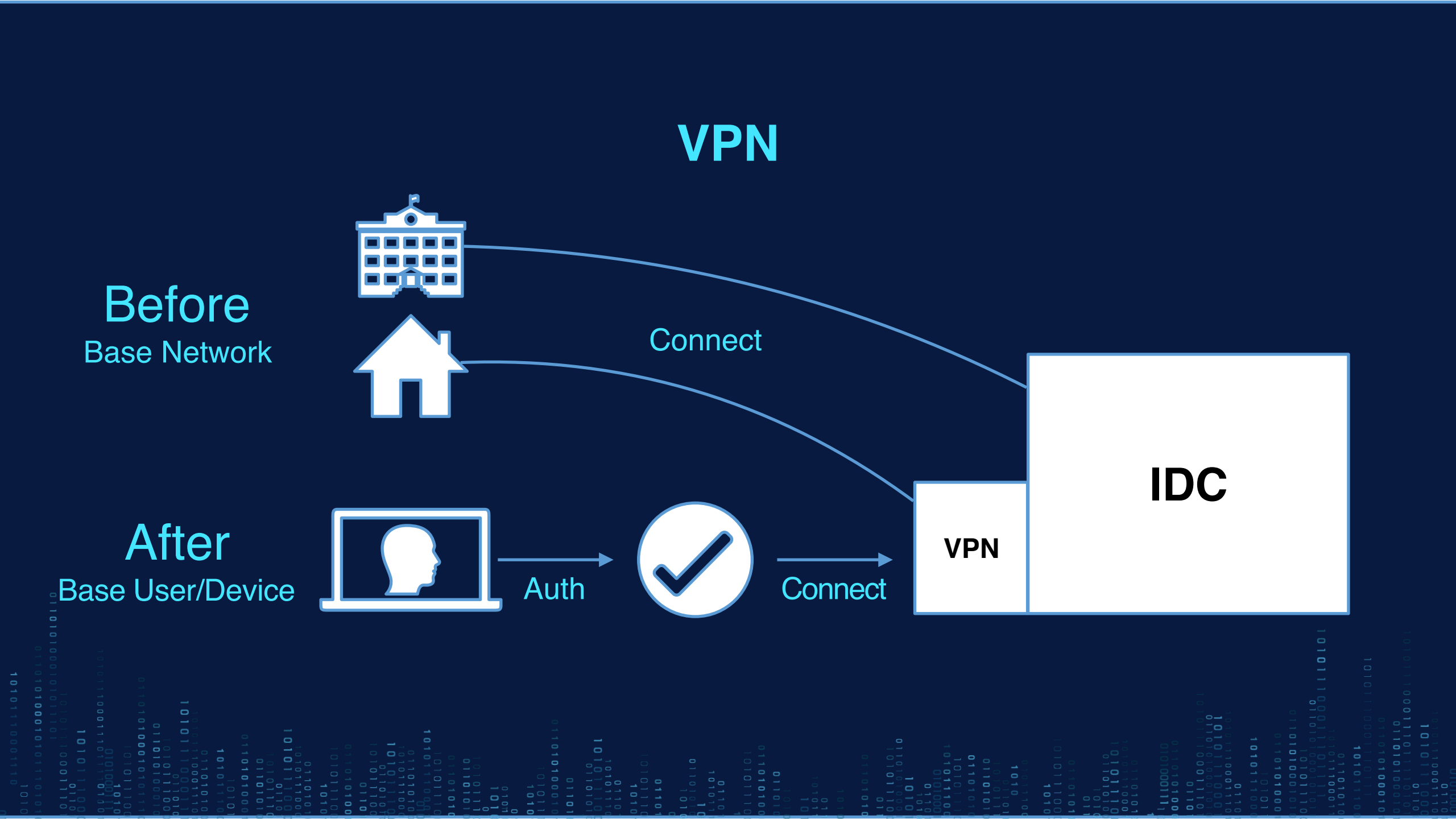
- Wi-Fi Attack
- VPN
- Username&Password

- Malware/Vulnerability
- LockScreen
- Security Config

One Client Solves All

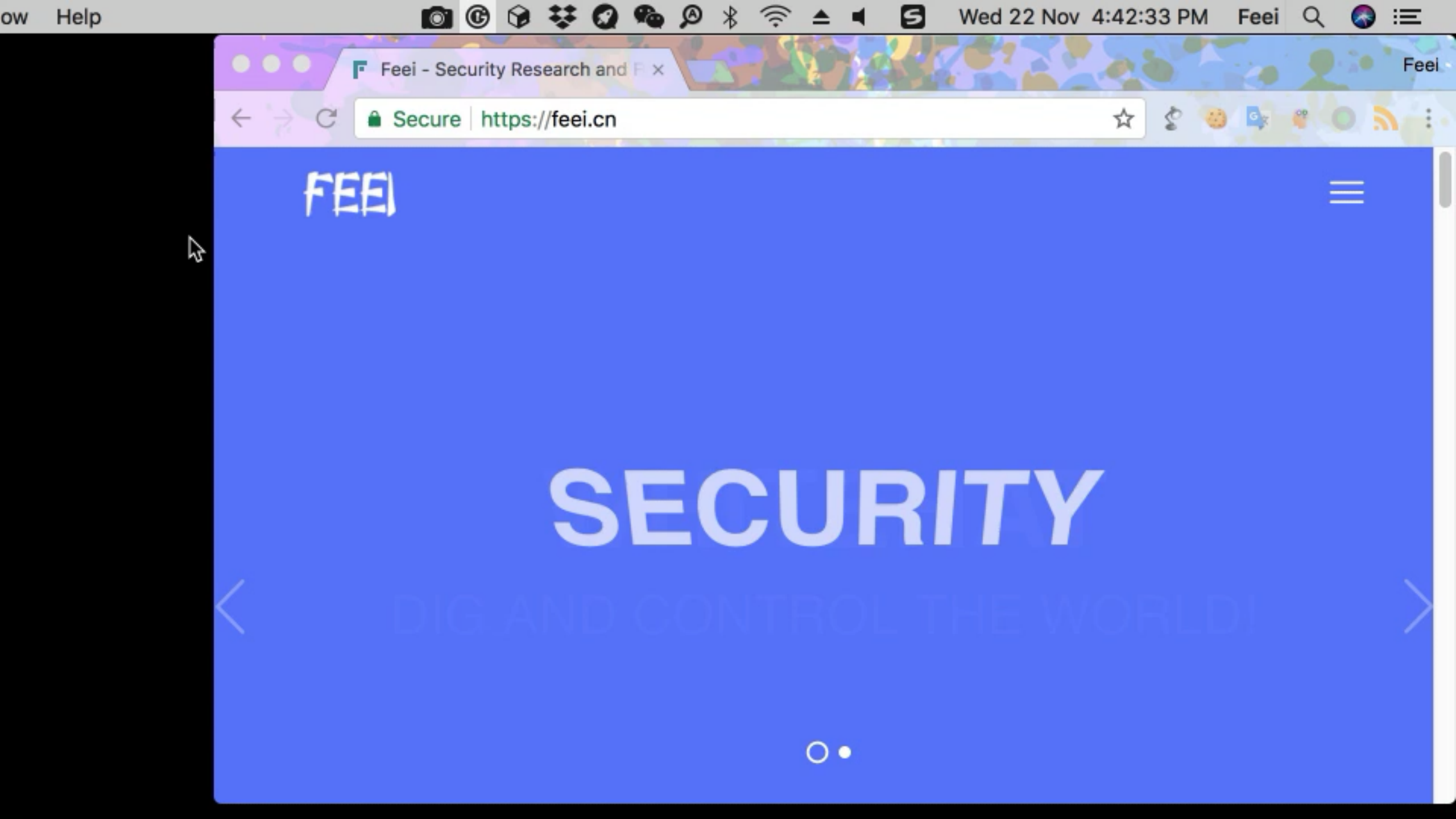


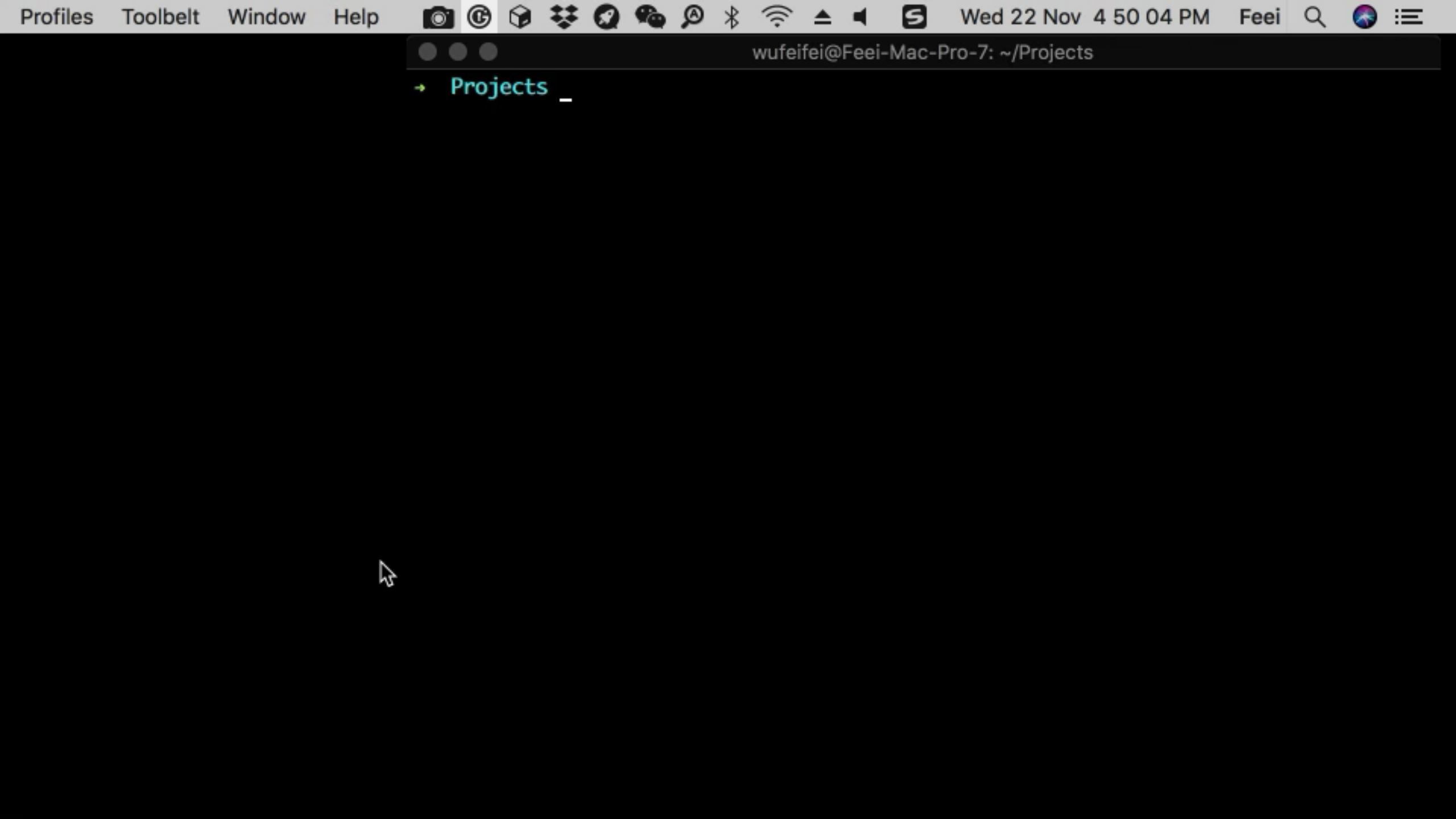
VPN


Before
Base Network
Connect
After
Base User/Device
Auth
Connect
VPN
IDC

Authentication Center

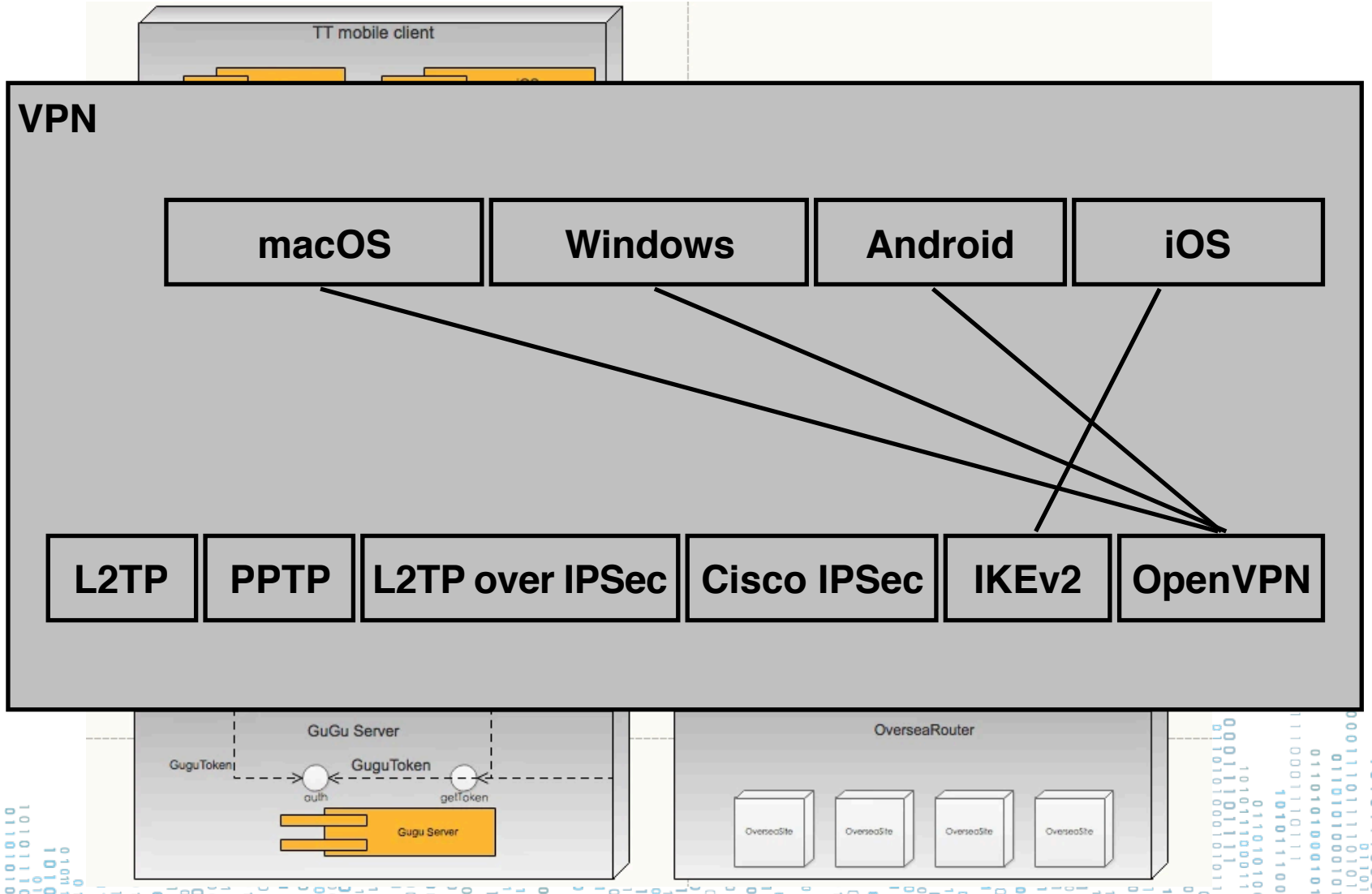

ow
Help
Wed 22 Nov 4:35:17 PM
Feei


ow Help
Wed 22 Nov 4:42:33 PM Feei
Feei - Security Research and
Feei
Secure https://feei.cn
FEEI
SECURITY
DIG AND CONTROL THE WORLD!


Profiles
Toolbelt
Window
Help
Wed 22 Nov 4 50 04 PM
Feei
wufeifei@Feei-Mac-Pro-7: ~/Projects
→ Projects

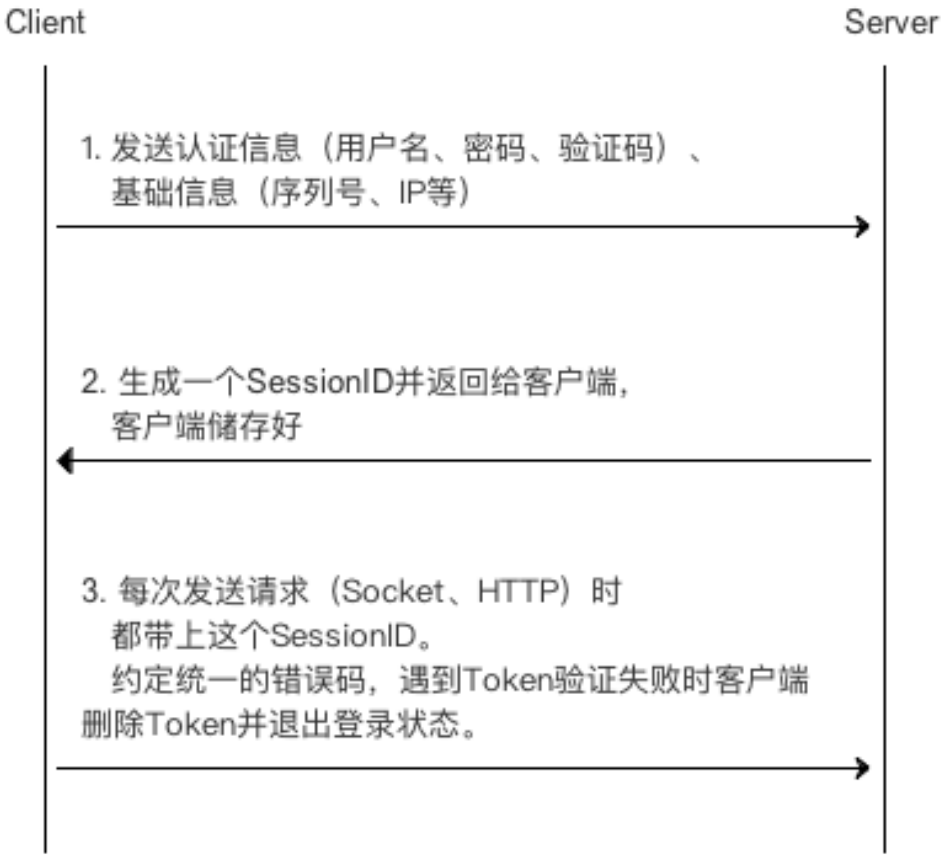
Difficulty 1：Cross Platform VPN

- Cross Platform
- Extensibility
- Stability
- Security



Difficulty 2：No-password for VPN

Token交互流程



Token生成规则

1. 随机数（客户端存储）
32位随机字符串（数字字符）

2. 防伪造（服务端存储）
随机数生成时和客户端传上来的序列号进行绑定

3. 标识用户（服务端存储）
随机数生成时和验证通过的UID进行绑定

4. 生效时间（服务端存储）
后台记录随机数的生效时间

Token失效规则

随机数不符合32位数字字符的规则
随机数不存在
随机数和序列号不是一对
随机数和UID不是一对
随机数生效时间超过7天

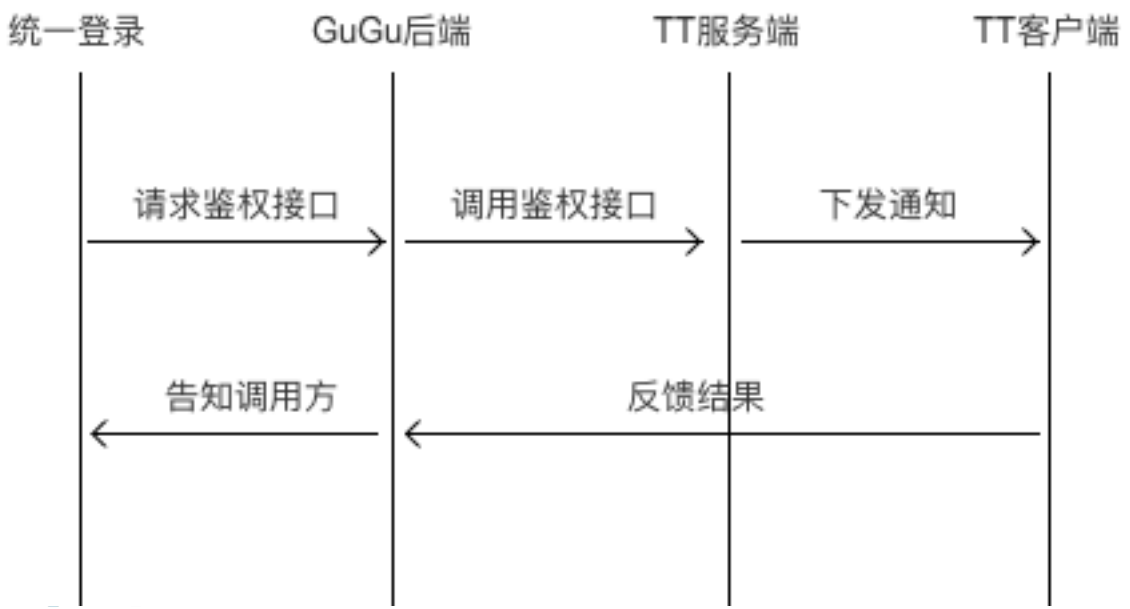
退出时删除随机数及对应信息

Difficulty 2：No-password for Web

Difficulty 2：No-password for Web

Difficulty 2：No-password for App

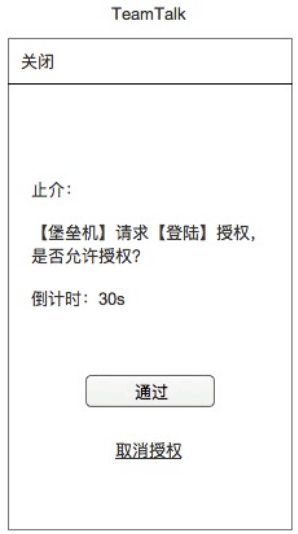
GuGu移动端免密鉴权方案



- 在手机浏览器中打开统一登录
- 统一登录根据User-Agent判断是手机
- 显示移动端一键登录的按钮
- 请求GuGu后端接口，拿到SUT(Single Use Token)
- 点击GuGu Logo

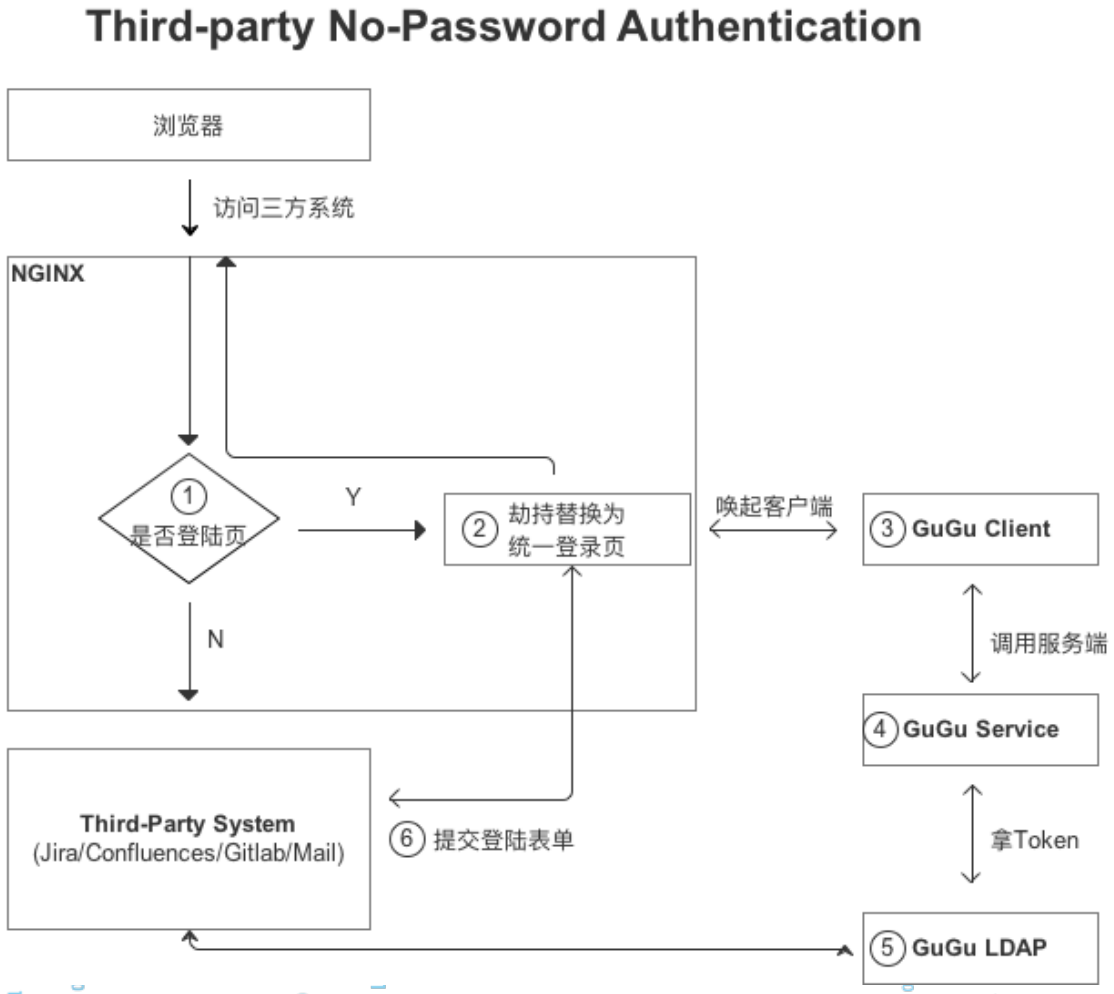
- 弹出加载中的浮层
- 通过iFrame加载Schema跳转到TeamTalk授权页
- Schema中附带了SUT

- 向GuGu后端轮询授权状态
- 授权通过则获取LoginToken
- 拿到LoginToken走登陆流程



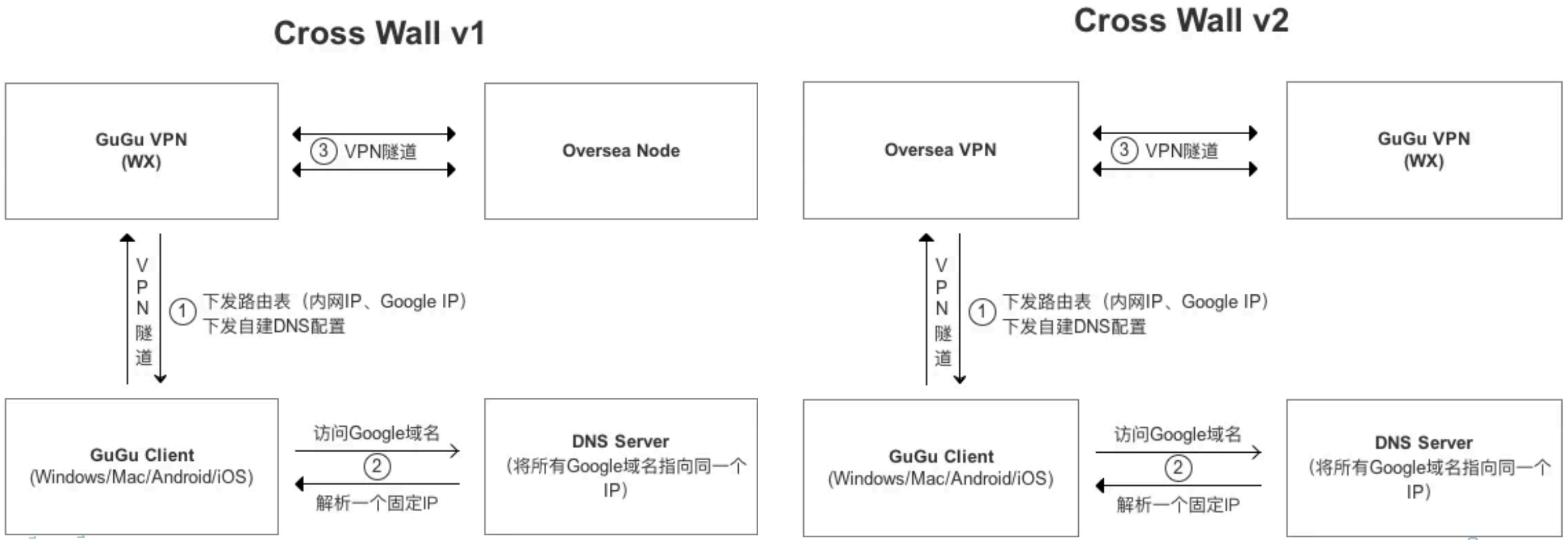
- 拿SUT找GuGu后端验证，若SUT不存在则不显示授权页
- SUT验证成功，则拿到【业务方】和【操作】并展示授权页
- 点击通过
- 调用GuGu后端接口，发送SUT+TT Token至GuGu后端
- GuGu后端将会向TT后端验证TT Token有效性，授权成功
- 关闭当前授权页面
- 唤起浏览器或引导用户返回打开浏览器

Difficulty 2：No-password for Third-party



GitLab Confluence Jira Software

Difficulty 3：Cross Wall



Difficulty 4：Malware

- Software Name
- Software Version
- Software MD5

DYLAN

- CVE
- Exploit-DB
- Blog/Site

Difficulty 5：Linkage

- SANGFOR
- Threadbook
- IDS
- Firewall
- Device Fingerprint
- Awareness Training


THANKS
Q&A