

专注终端安全 保护核心机密 **BEST CHOICE**

IP-guard&深信服

VPN终端管理安全加固方案

VPN安全加固的背景

内外网的边界模糊化

- 员工的办公地点**多样化**
- **交互时段**超越工作时间
- 员工**全时段**接触内网
- 内网边界开始**往外延伸**

绝对的信任不复存在

- 攻击和**泄露事件**在增加
- 大量存在的**身份盗用**
- **不安全**的人、用户和设备
- 企业急需**重构**信任的基础

零信任的安全模式

- 现有安全机制**不够安全**
- 我们选择**不相信**任何人
- 在**明确授权**下，并接受**完**
全审查才能访问内网资源
- **信任关系**需要重新构建

VPN安全加固的背景

等保2.0 新增的 重要要求项

- 安全审计：应确保审计记录的留存时间符合法律法规。
- 具体要求：应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

出自等保第三级→安全通用要求→8.1.3 安全区域边界→8.1.3.5 安全审计

等保2.0 框架和思路 的变化

- 原来等保1.0没有完整的体系思路，以单点的、被动防御为主。
- 现在等保2.0变成了事前，事中，事后，防不住要审计，出现问题还可以事后溯源，是一个整体化的体系进行分类管控。

VPN安全加固的背景



法律条款



- 第二十一条规定：保障网络免受干扰、破坏或者未经授权的访问，**防止网络数据泄露或者被窃取、篡改**



《网络安全法》

- 第二十一条 防止网络数据泄露或者被窃取、篡改
- （四）采取数据分类、重要数据备份和**加密**等措施

法律条款



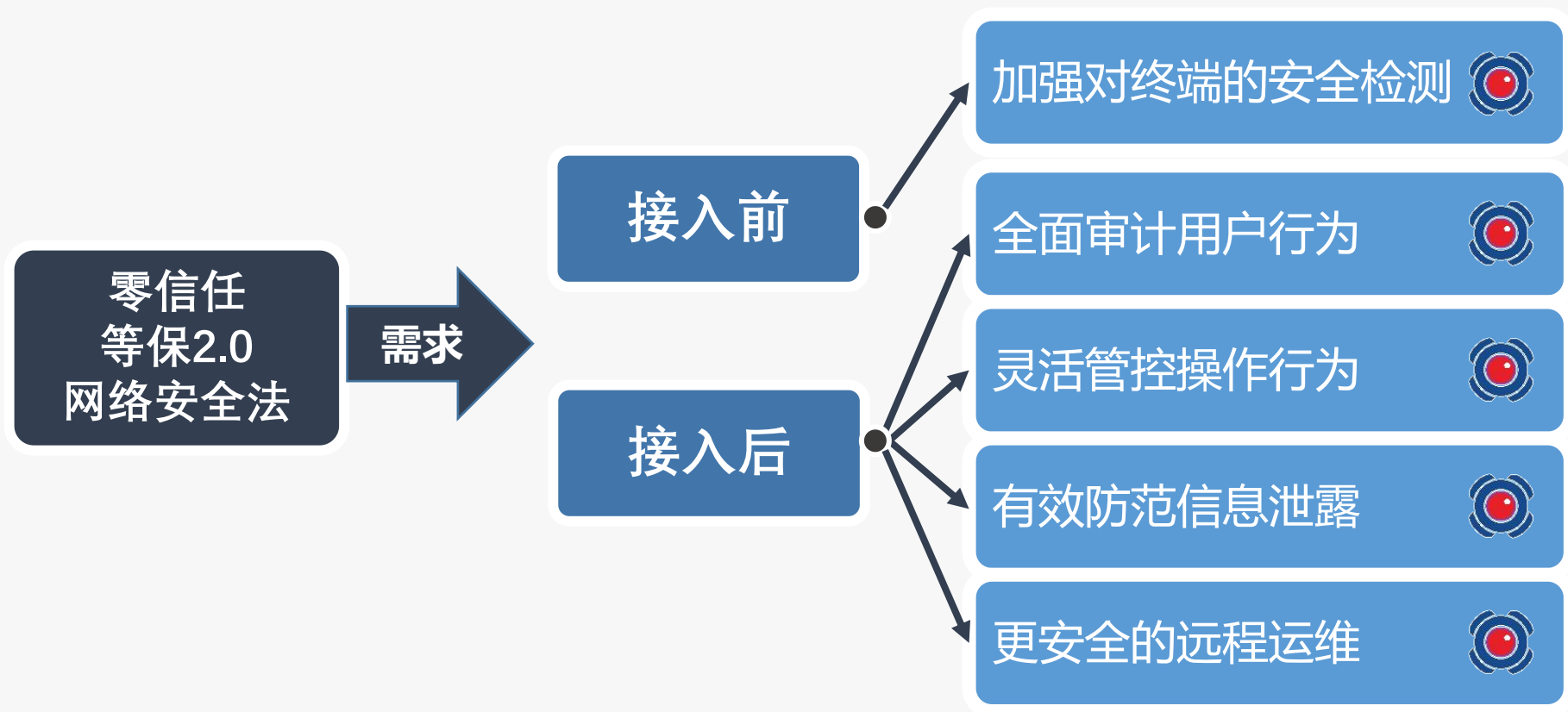
第四十二条

- 网络运营者应当采取技术措施和其他必要措施，**确保**其收集的个人信息安全，**防止信息泄露、毁损、丢失**



法律条款

VPN终端管理安全加固五大需求



VPN安全加固方案的全局视图



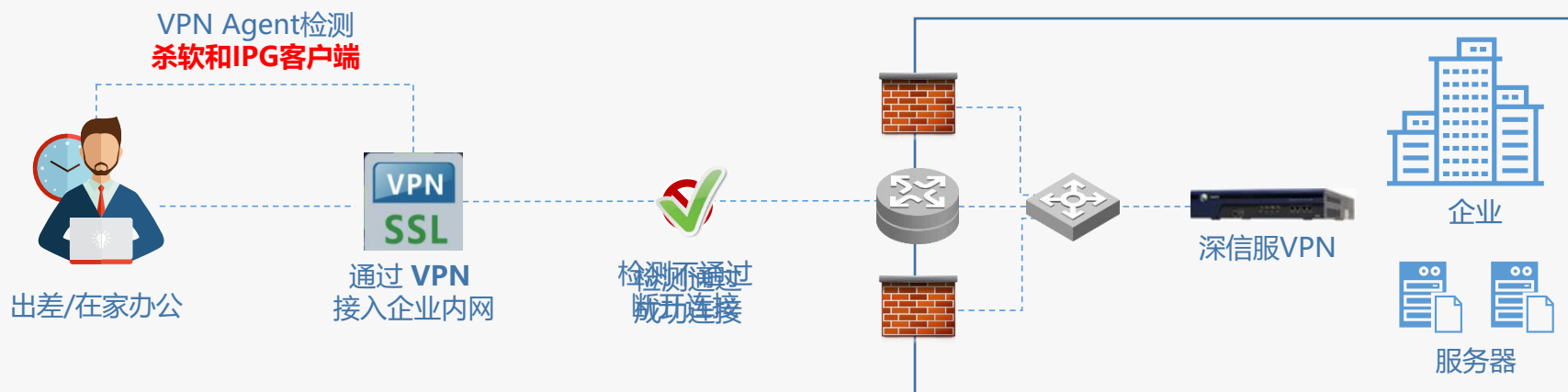
VPN终端管理 安全加固方案



场景一：VPN接入前的主机安全检测

场景需求描述

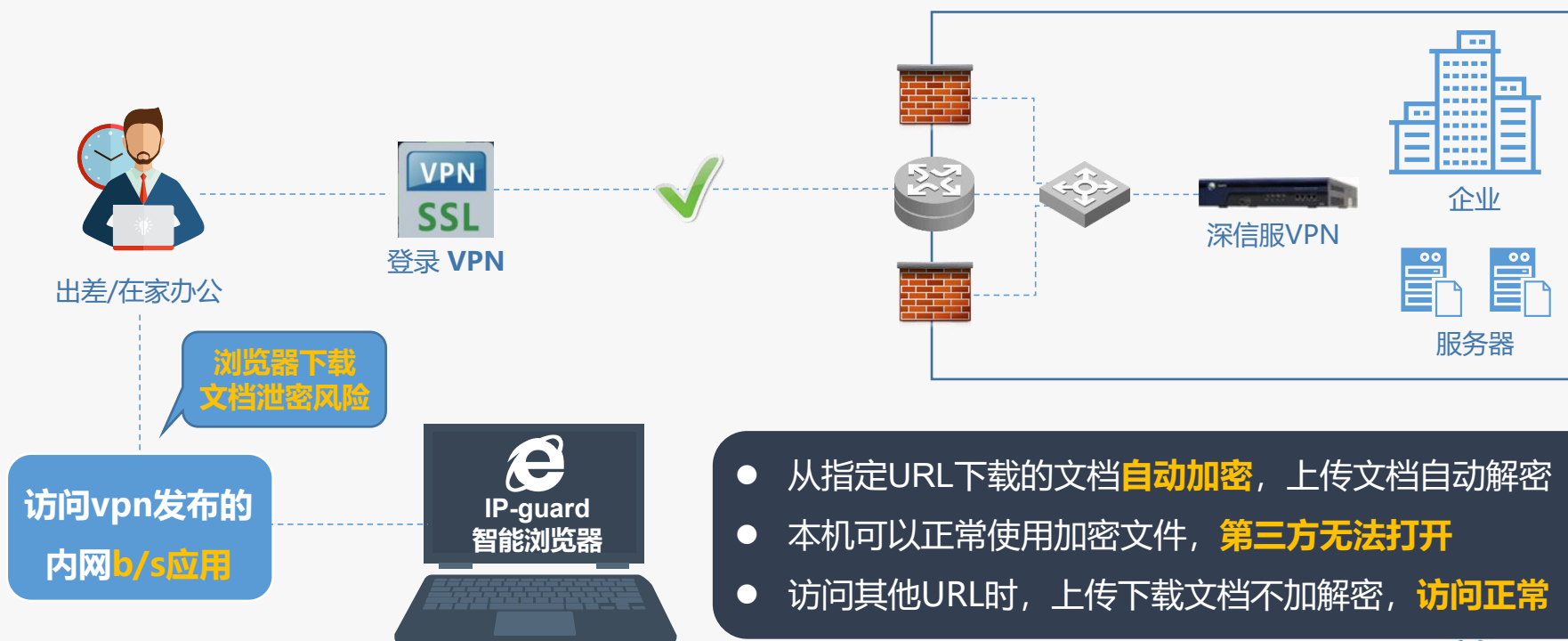
在“零信任”理论的安全发展趋势下，外部计算机通过VPN接入可能会带来安全风险，需要更严格的接入安全检测，实现更有效的“身份认证”



场景二：VPN接入后文档下载加密保护

场景需求描述

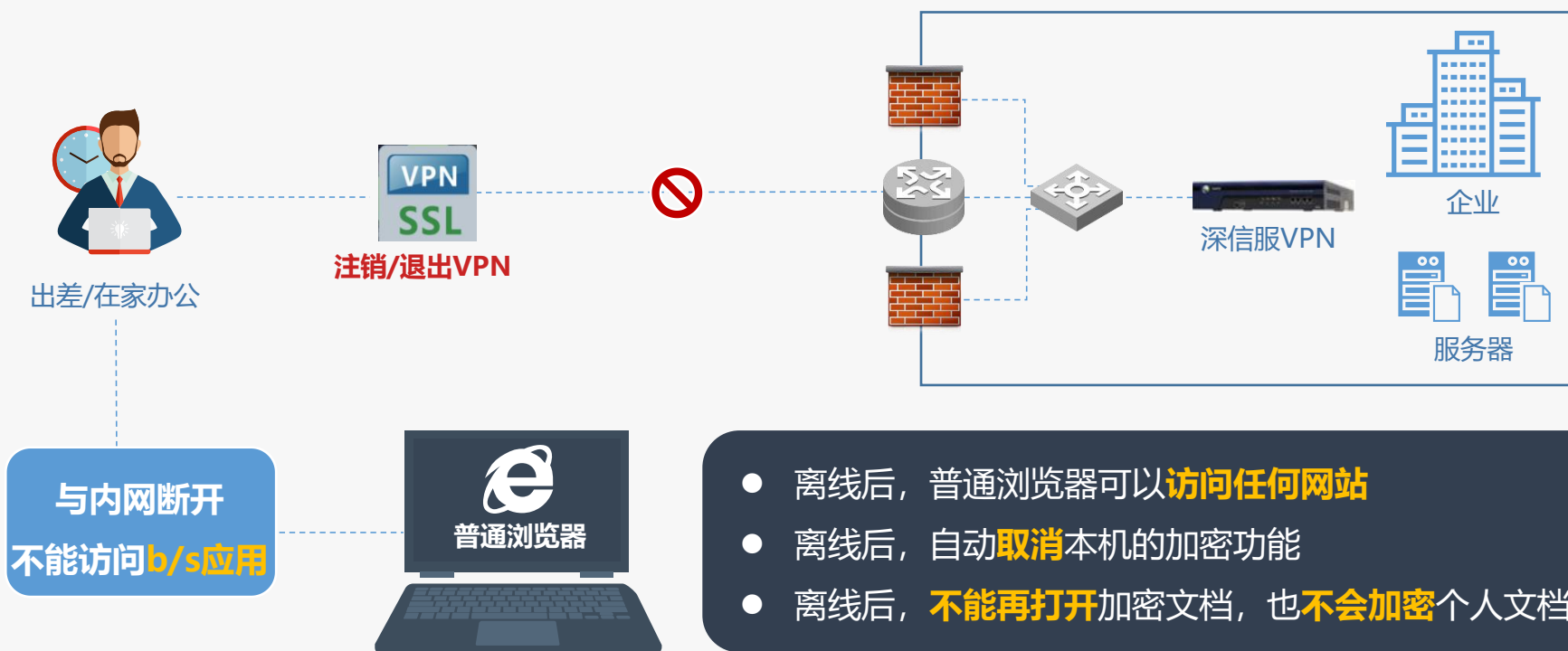
VPN用户远程接入企业内网后，有可能会直接从重要的业务系统下载资料到本地电脑，有很大的重要数据信息泄露的风险，需要对下载文件进行加密，实现有效的“事前防护”



场景二：VPN接入后文档下载加密保护

场景需求描述

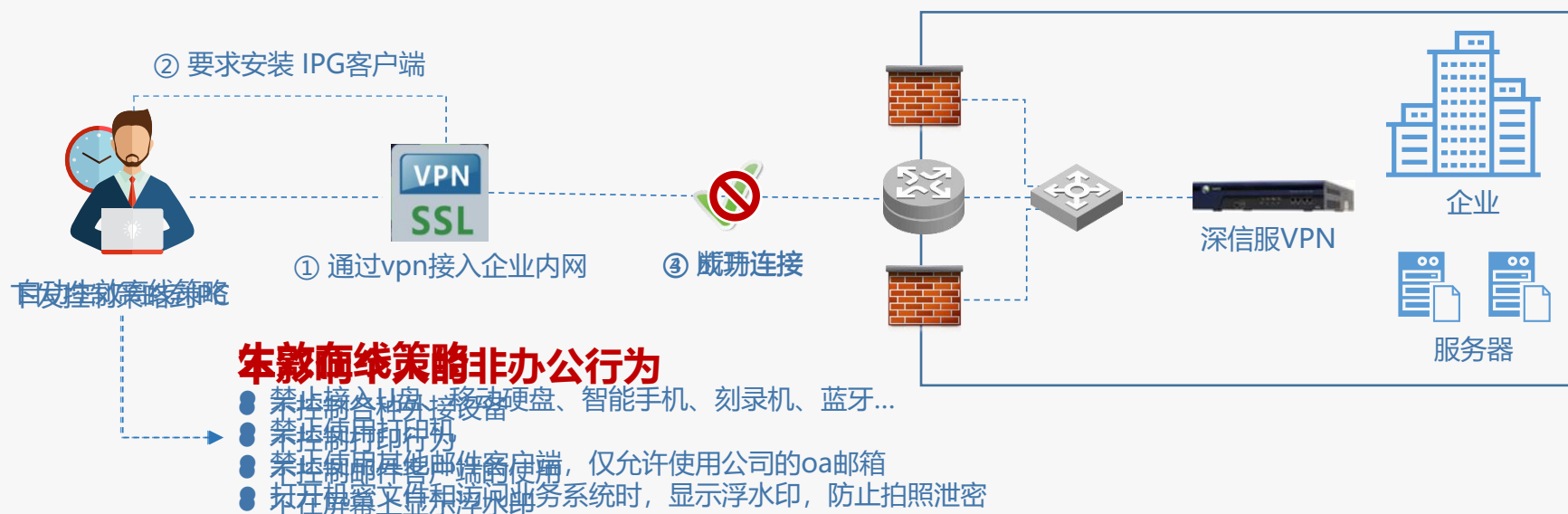
VPN用户远程接入企业内网后，有可能会直接从重要的业务系统下载资料到本地电脑，有很大的重要数据信息泄露的风险，需要对下载文件进行加密，实现有效的“事前防护”



场景三：VPN接入后的用户操作管控

场景需求描述

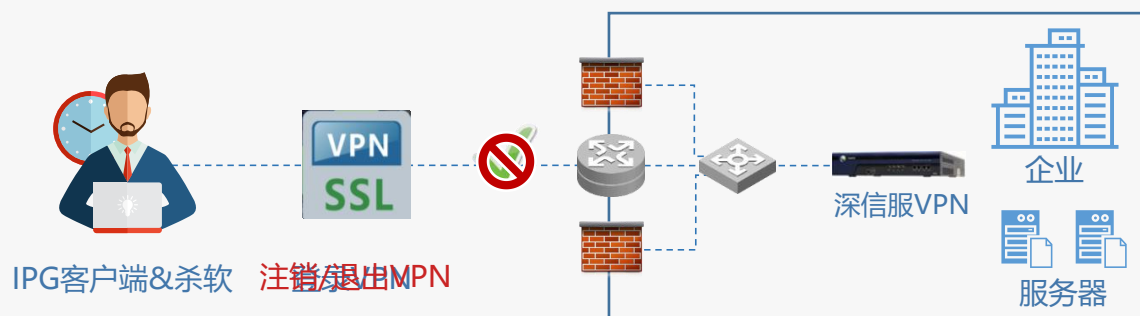
对接入的终端计算机进行必要的权限控制，避免因为用户随意访问或者下载带来安全风险，有效的实现“事中控制”。



场景四：VPN接入后的用户行为审计

场景需求描述

对用户访问内网的行为进行全面记录，有效实现事前震慑与事后追溯，实现有效的“事后审计”

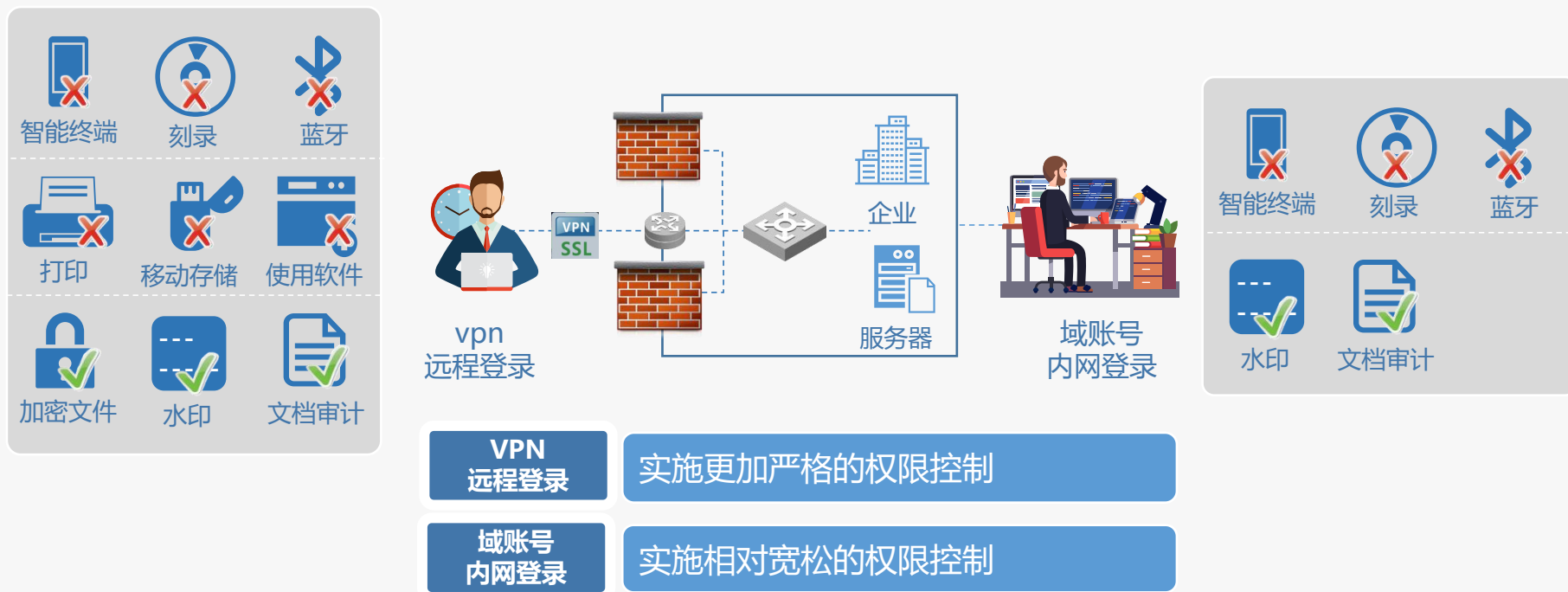


- 记录文档操作的全生命周期
- 与日志记录有关的功能自动取消，不记录个人操作行为
- 外接设备的使用日志

场景五：对同一个用户账户的智能区分

场景需求描述

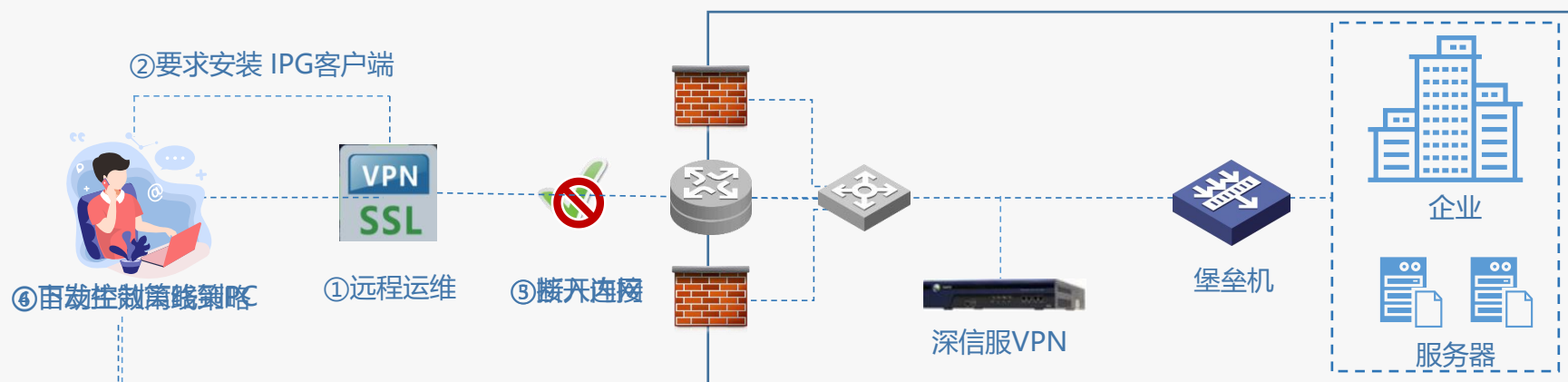
使用同一个域账号，在两种接入状态下（vpn远程接入/在企业内网接入）自动进行智能区分，执行有差别的控制策略，实施灵活有效的安全管理



场景六：更安全的堡垒机接入场景

场景需求描述

更好的提高远程终端通过VPN接入堡垒机的安全性，降低因违规运维操作导致的泄密风险



策略控制策略策略

- 禁止接入各种外接设备、智能手机等外接设备
- 远程运维时显示屏显示浮水印，防止拍照泄密
- 实时录制屏幕操作画面，记录运维操作

方案总结

实现 闭环管理

接入之前--进行更严格的**身份认证**

文档加密--实现有效的**“事前防护”**

权限管控--实现灵活的**“事中控制”**

操作记录--实现全面的**“事后审计”**

实现 法规要求

- 满足 **“等保2.0”** 关于远程访问**安全审计**要求
- 满足 **“网络安全法”** 关于**信息防泄漏**的要求
- 符合 **“零信任”** 的网络安全**发展趋势**

VPN安全加固组件功能明细

VPN审计管 控组件

基本模块，打印管控，设备管控，
应用程序管控，网页浏览管控，
屏幕监控，网络管控，邮件管控，
即时通讯管控，文档操作管控，
移动存储管控，慧眼风险审计报告

VPN文件加 密组件

文档透明加密



专注终端安全 保护核心机密

Copyright © 2001-2017 TEC Solutions Limited. All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. IP-guard may change the information at any time without notice.