奇安信 | 新一代网络安全领军者

上网行为管理

奇安信认证培训中心

上网行为管理设备

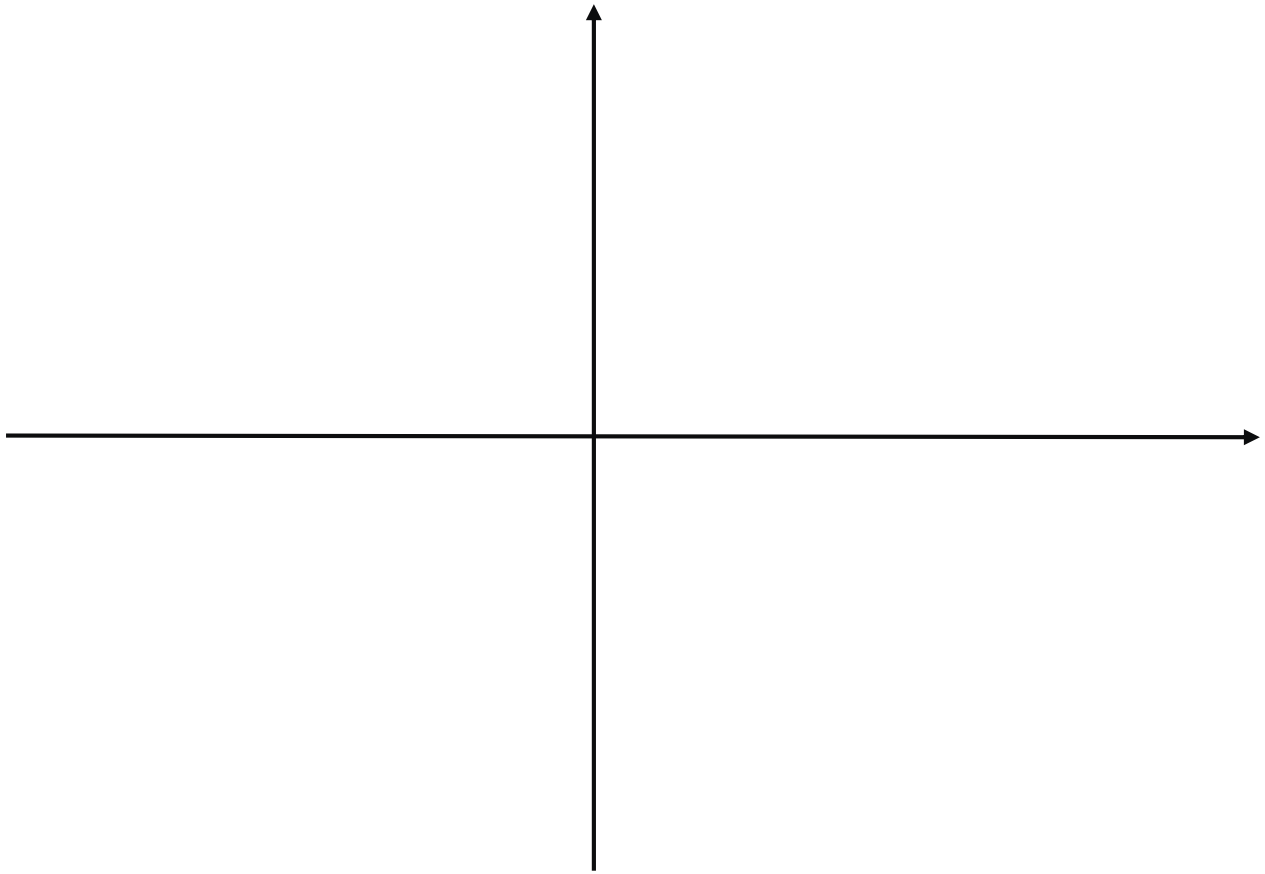
什么是上网行为管理系统?

- 软硬件一体化设备
- 常部署在网络边界
- 可对企业内部员工的上网行为进行全方位有效管理

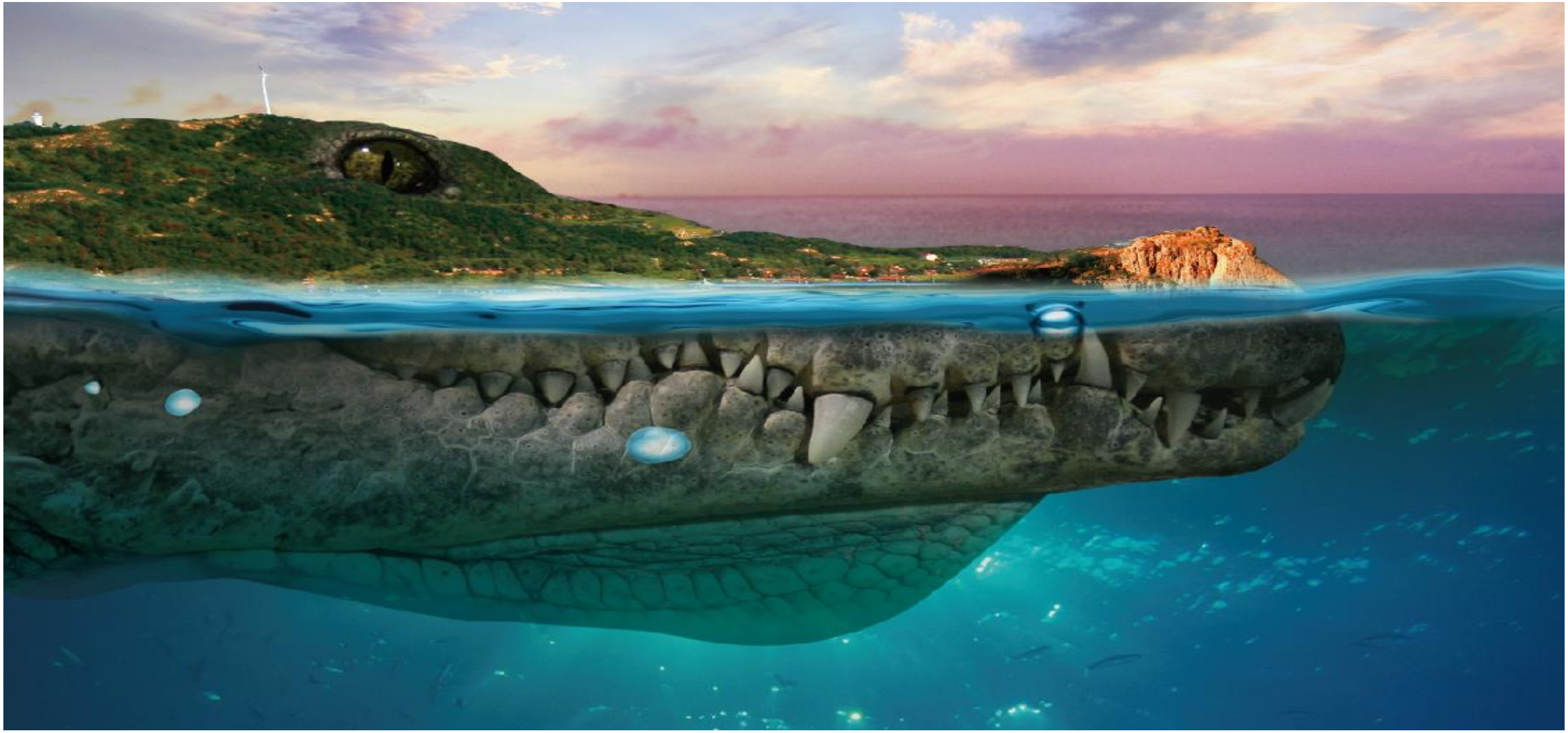
ICG，Internet Control Gateway的缩写，产品名称。

本门课以ICG代称 奇安信上网行为管理产品。

上网行为管理设备的诞生，是为了应对 企业员工 上网时产生的各种安全风险和合规隐患。



看似平静的互联网，暗藏风险重重



技术创新生生不息，上网风险如影随形

应用云化，监管盲点

安全风险

移动应用，更新频繁

效率风险

数据价值，亟待挖掘

钓鱼勒索，防不胜防

法律风险

加密管控，缺乏手段

安全风险

恶意网址

- 浏览器网站访问
- 邮件正文链接
- 社交软件聊天链接

恶意软件

- 浏览器文件下载
- 网盘文件下载
- 社交软件文件传输
- FTP文件下载
- P2P文件下载

信息泄露

- 邮件外发信息
- 论坛社区上传
- 云笔记、网盘上传
- 社交软件聊天

违反规定

- BYOD设备上网
- 不合规电脑上网
- 私接Wi-Fi外连
- 加密应用逃避监管

效率风险

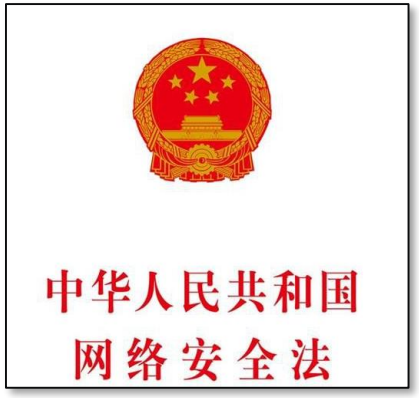
工作无关应用降低工作效率

- 沉溺网络游戏
- 无节制IM聊天
- 频繁网络购物
- 炒股炒币挖矿

工作无关下载消耗带宽资源

- P2P影视下载
- 网络直播视频
- 大文件共享传输

法律风险



《中华人民共和国网络安全法》

- 第十二条 任何个人和组织 … 不得利用网络从事宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。
- 第二十一条 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。
- 第五十九条 不履行本法第二十一条 … 规定的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

《公共场所无线上网安全管理要求》

- 向公众提供Wi-Fi无线上网服务的公共场所，应依法向公安机关登记备案，落实上网实名认证、上网行为审计、日志留存等网络安全技术措施，安装已取得公安部相关销售许可证的网络安全管理系统并联网运行。
- 对拒不履行的场所责令整改后仍未整改的，公安机关可以依法予以警告、罚款、停机整顿等处罚。

上网行为管理产品的前世今生

- 有人认为，上网行为管理产品就是流控产品的加强版。
- 从产品发展的纵向角度看，上网行为管理产品和网络安全审计产品之间才是真正的传承关系，它们技术上有共同的特点，就是数据收集。

演变改革

流量识别方法改进

对流量的识别方式，从基于端口过度到基于应用协议，跟上了网络应用的发展潮流

策略作用对象改进

作用对象从IP到自然人的变化，可以与用户的组织结构对应融合，使策略与报表的描述变得更加贴近于管理流程

作用层面改进

上网行为管理的作用层面从事后向前拓展至事中，变成了对IT和管理起到辅助作用的产品，而不再仅仅是一款保证合规性的产品

上网行为管理产品的归类

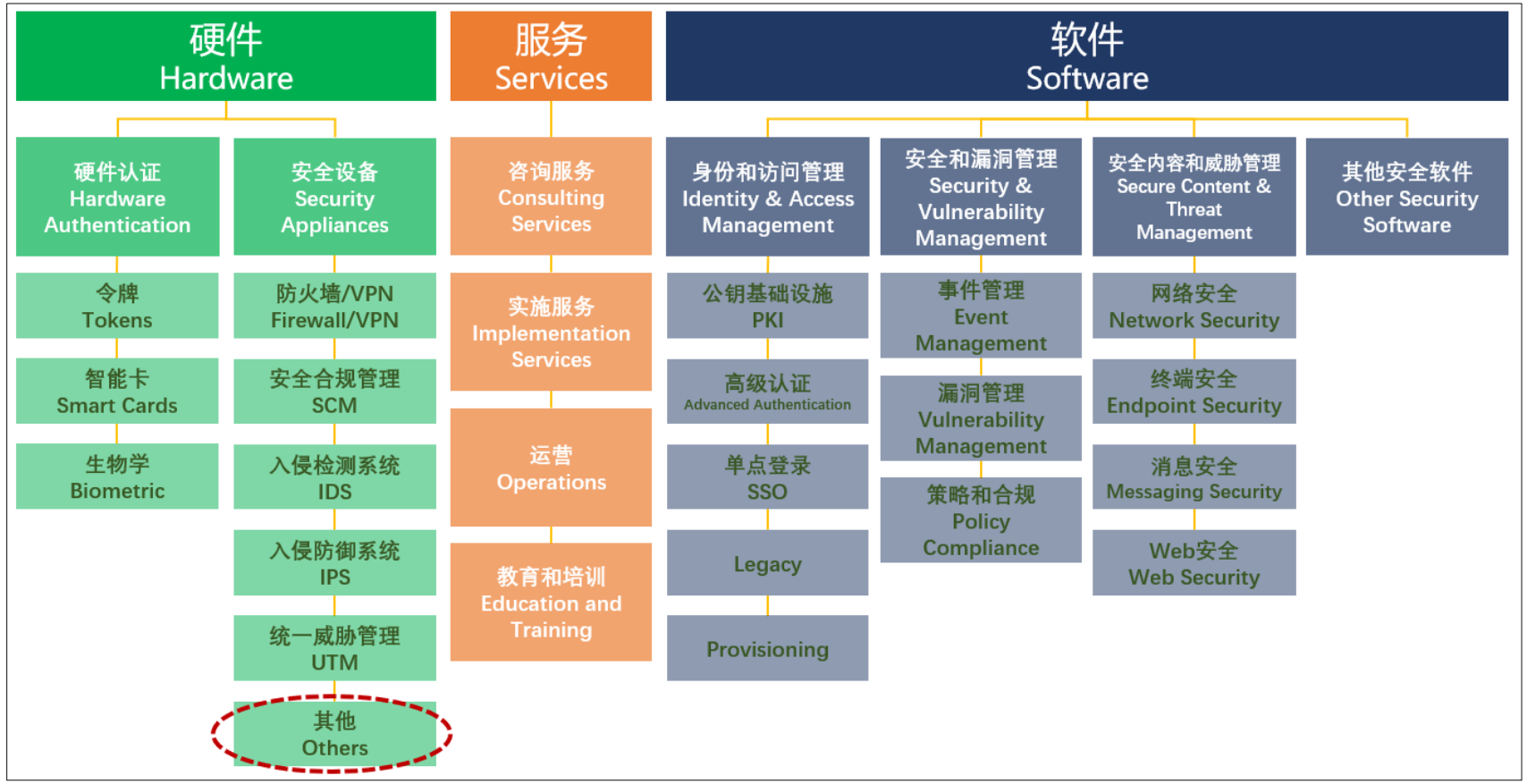
- 国际知名权威信息技术研究和分析公司Gartner也没有对上网行为管理（Network Behavior Management）这一产品的分析和研究，与其最接近的是安全Web网关（SWG，Secure Web Gateway）品类。
- 大家可以简单的理解为与中国的上网行为管理产品相对应的国际化产品为安全Web网关（SWG）。

上网行为管理产品的归类

- Gartner对于SWG的产品定义为：强制执行基于应用和网站服务的流量检查，防止恶意软件攻击，并支持或集成数据丢失防护功能，用来保护用户免受互联网带来的威胁，并帮助企业满足政策合规性要求，并给出了SWG产品品类的必备和可选特性。

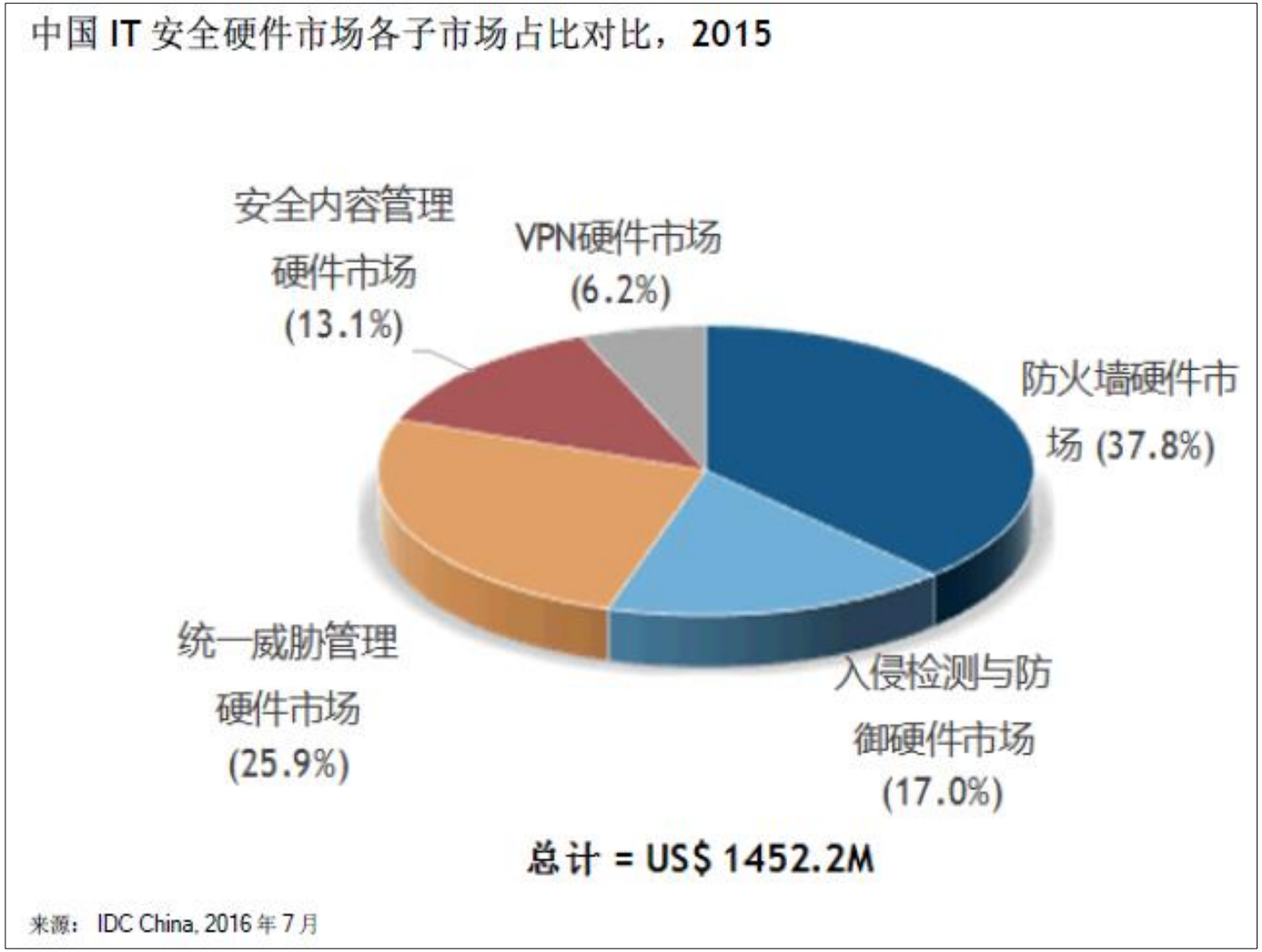
上网行为管理产品的归类

- IDC在2015年6月发布的《中国IT安全硬件、软件和服务2015-2019全景图》报告中对信息安全产品的分类。在这个分类体系中没有明显的上网行为管理产品或SWG品类，但从产品功能角度考量，行为管理类产品与入侵检测（IDS）、入侵防御（IPS）最为接近，因此只能将其分在安全设备的“其他”之中。



上网行为管理产品的归类

- IDC在2016年7月发布的《中国网络安全市场份额，2015：IT安全硬件、软件、服务》报告中，将中国IT安全硬件市场分为安全内容管理、VPN、防火墙、入侵检测与防御和统一威胁管理五个子市场。此后发布的各类报告也都保留了安全内容管理这一大的分类，上网行为管理产品属于这个分类。



上网行为管理产品的归类

交通行为管理

交警在路口设卡，可以做什么？

记录：人员信息、车辆信息、运输货物信息、去往目的地

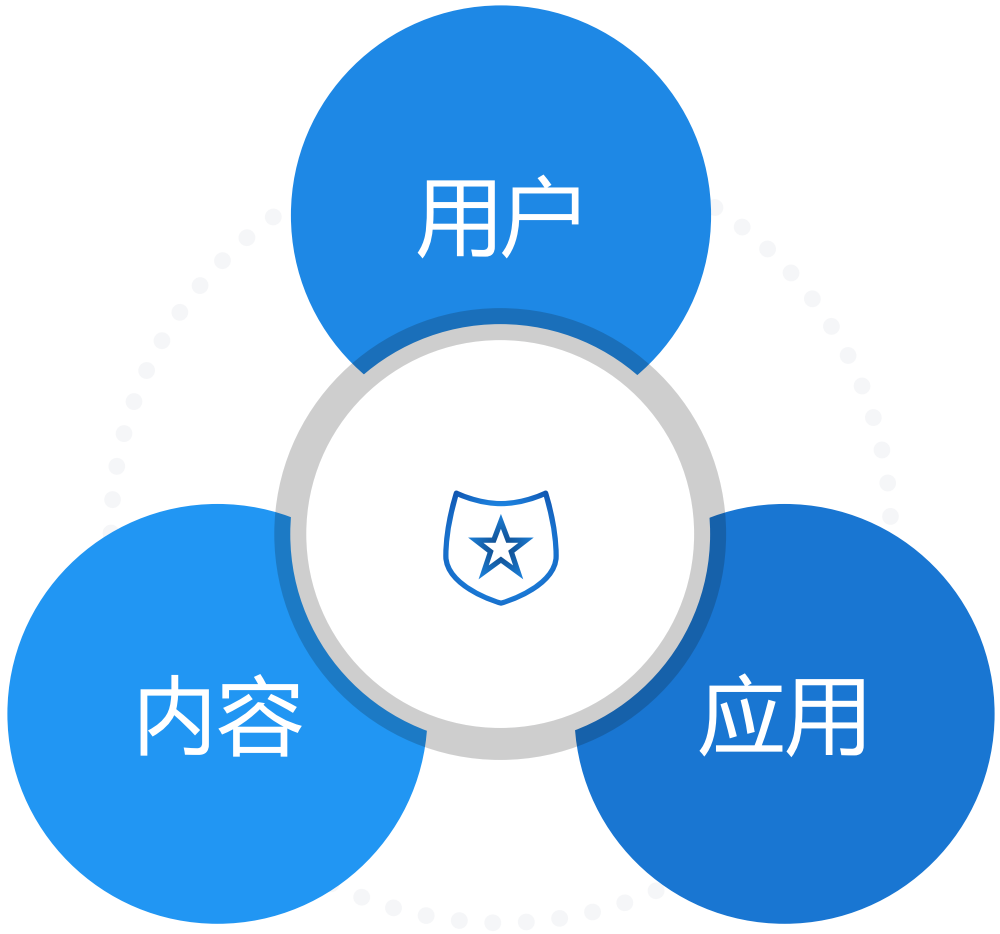
拦截：违法人员、违法车辆、违法货物等

管制：限速限流

ICG就是网络世界的“交警”，
在通向互联网的路口设卡拦截。

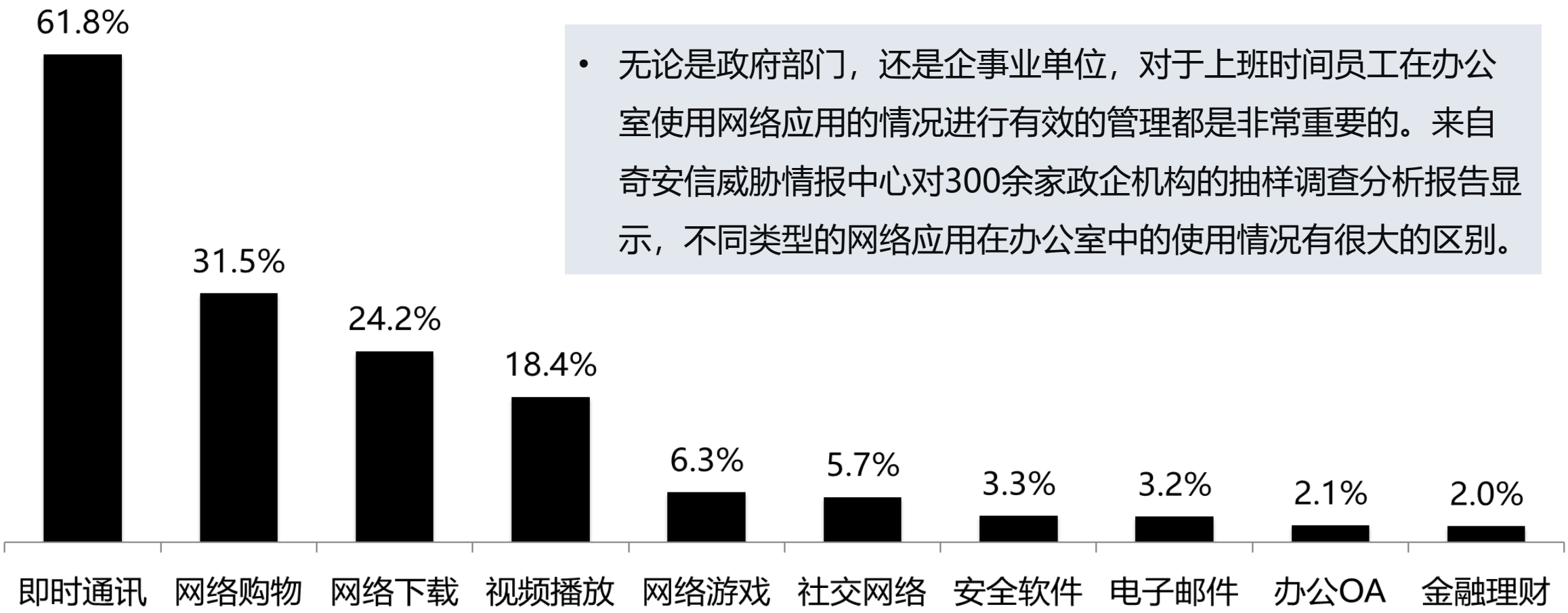
行为安全与上网行为管理

上网行为管理产品是一种对人的上网行为进行管理的网络设备，它基于应用层流量识别与数据采集技术，可对上网行为进行控制、审计与管理，提供了包括网页访问管理、网络应用管理、带宽流量管理、信息收发审计等功能。此外，该产品能够基于审计数据对人的行为进行查询、统计、分析和挖掘，帮助用户有效管理和使用网络。



网络资源的科学管理

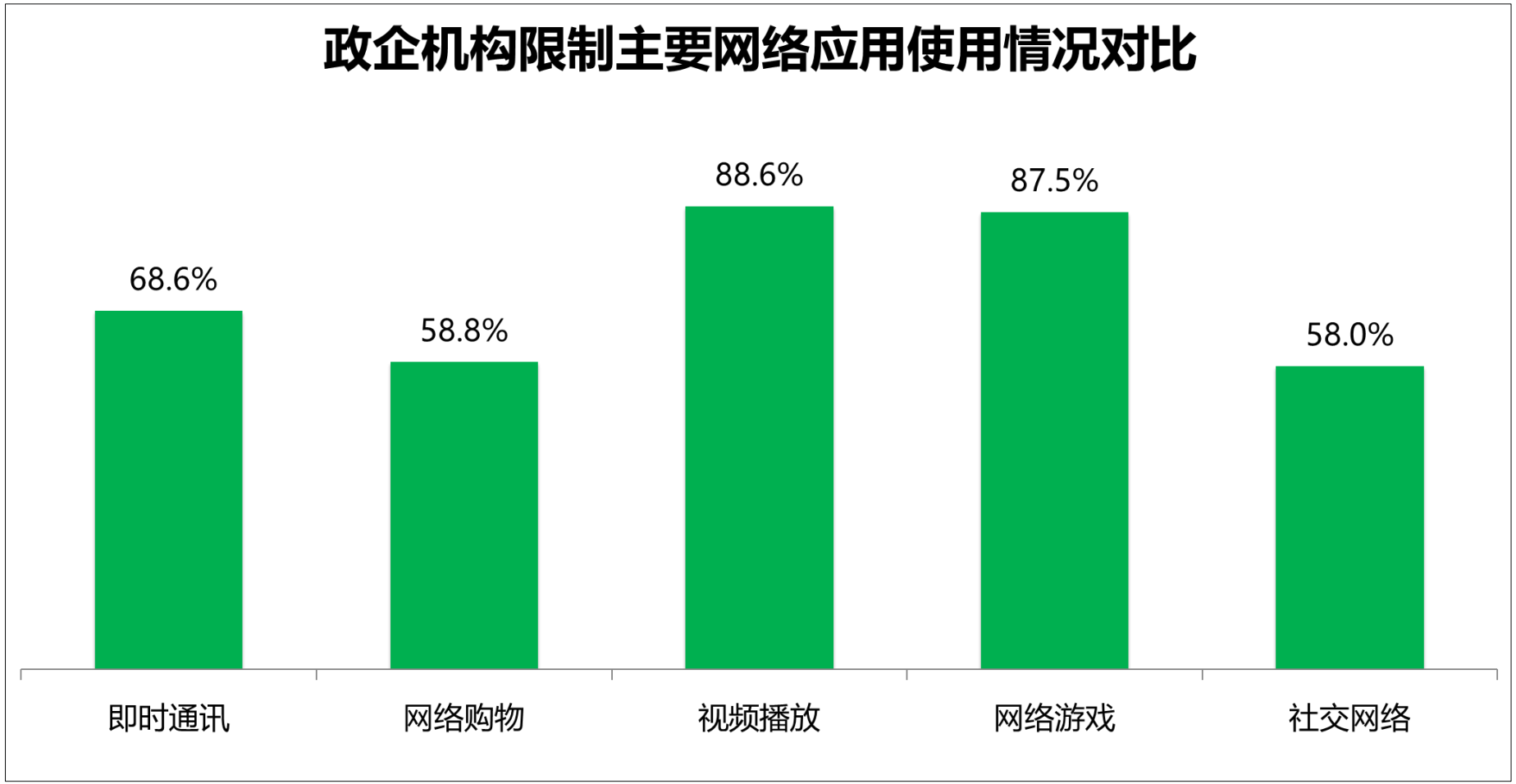
办公室里员工使用比例最高的十大网络应用



- 无论是政府部门，还是企事业单位，对于上班时间员工在办公室使用网络应用的情况进行有效的管理都是非常重要的。来自奇安信威胁情报中心对300余家政企机构的抽样调查分析报告显示，不同类型的网络应用在办公室中的使用情况有很大的区别。

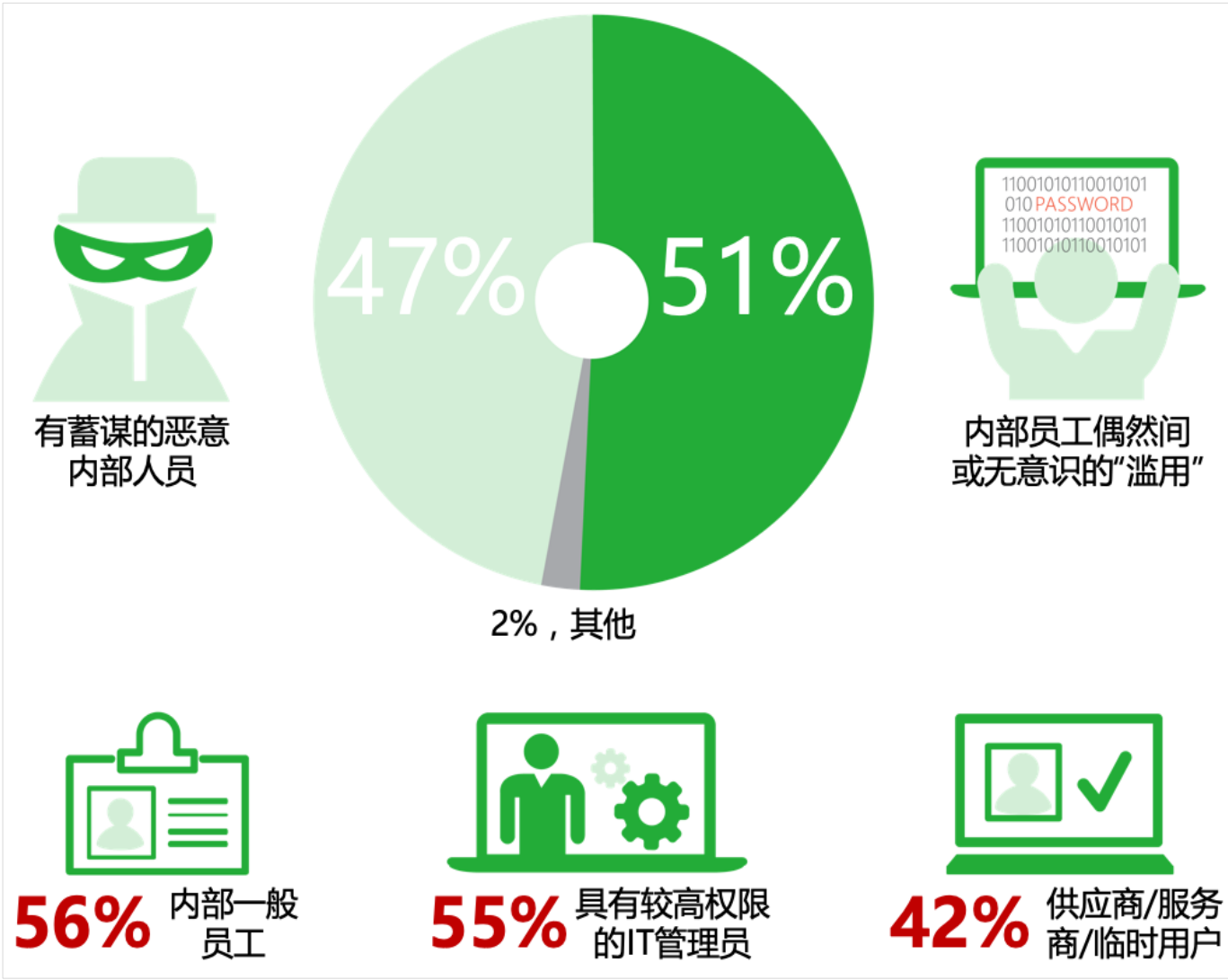
网络资源的科学管理

- 正因如此，为了能够提高网络使用率，提高员工工作效率，很多政企机构目前都已经开始部署和使用行为安全管理（上网行为管理）设备，在企业网络边界上对特定网络应用进行限制和拦截。



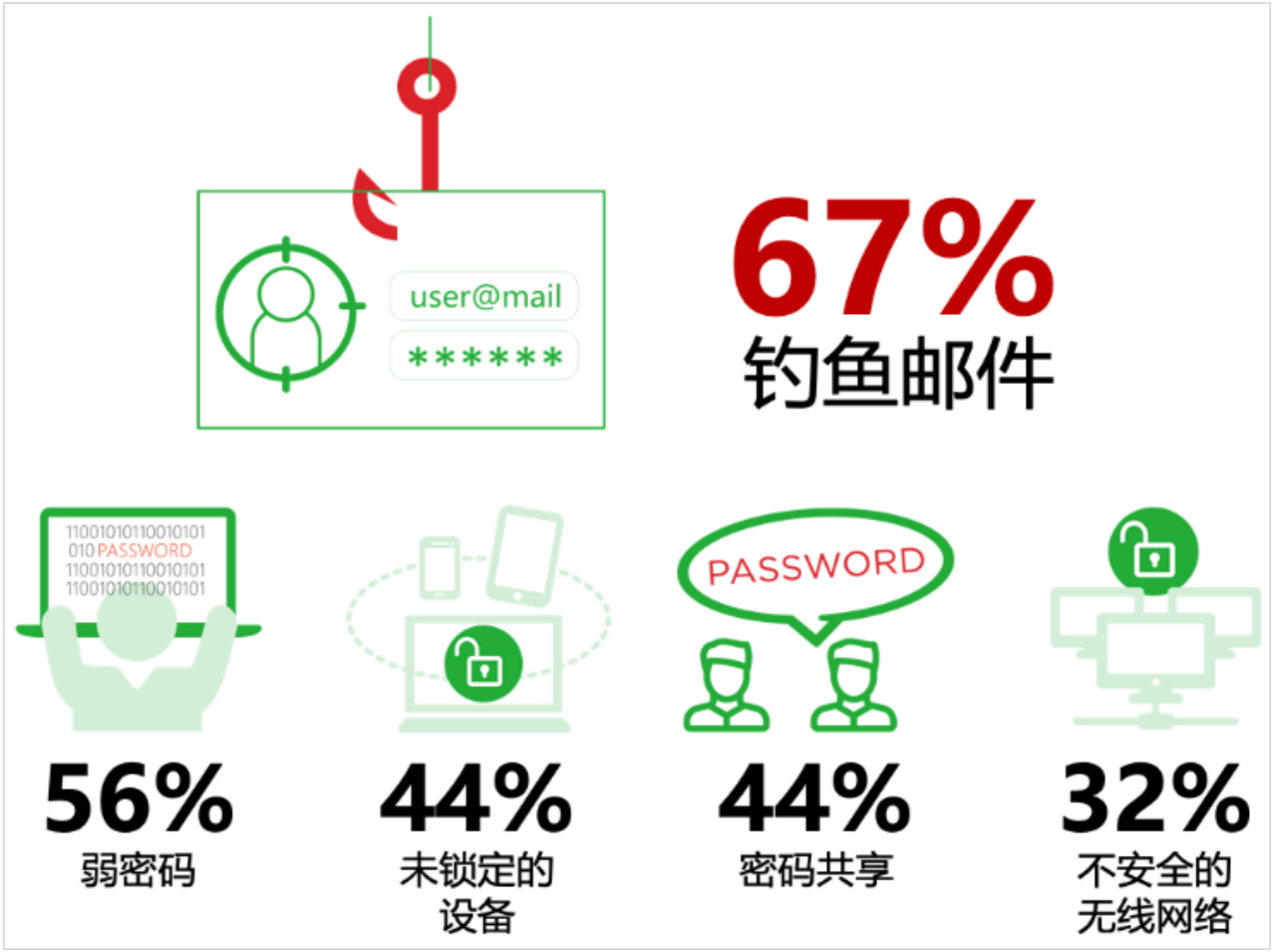
内部威胁及业务风险的发现与防范

- 有调查数据显示，内部威胁已成为当前企业网络安全的最大危害。通过对400,000名企业信息化管理者的调查显示，51%的管理员认为内部威胁主要产生于内部员工偶然或无意识的“滥用”，相比之下47%的管理员认为内部威胁更多来自于有蓄谋的恶意内部人员。
- 所谓“内部人员”包括了供应商、外包商、内部一般员工、IT管理员等



内部威胁及业务风险的发现与防范

- 造成内部威胁的行为或风险因素很多，以往绝大多数的安全设备（如，下一代防火墙、IDS/IPS、WAF等）及安全措施都是用来防范“外敌”的，而往往对这些内部威胁的高风险因素不起作用。
- 行为安全管理设备好比“数据探针”，可以识别人的违规或恶意操作。收集内网用户访问外部互联网、内部各种业务系统、数据库和服务器的数据，从业务系统、业务操作和内部人员三个维度构建行为基线和评分，帮助信息化管理员掌握各种网络系统的整体态势。



法律风险的有效规避

- 部署行为安全管理设备的另一个重要价值就是帮助组织有效的规避由用户非法访问互联网而带来的法律风险。
- “提供非经营性上网单位必须落实互联网安全保护技术措施，安装经网络监管部门检测通过的专用审计设备。”

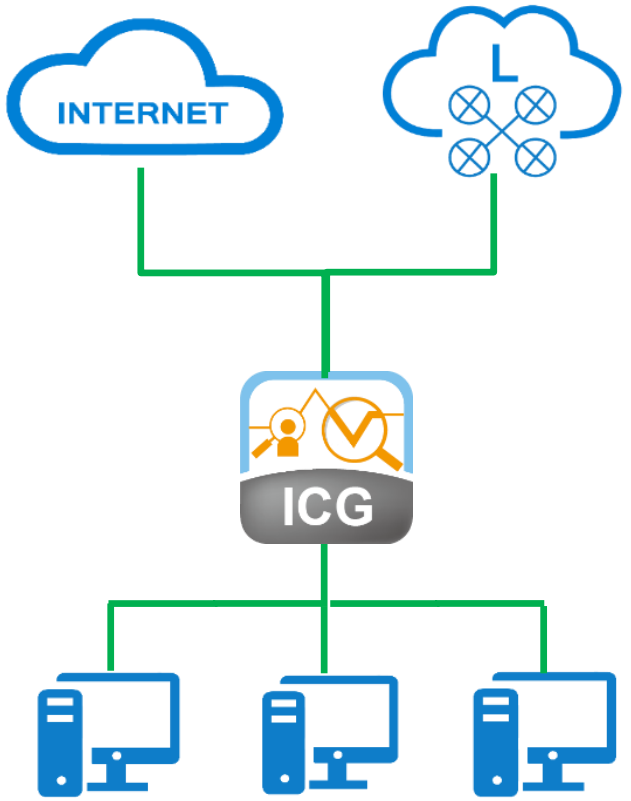
上网行为管理（ICG）简介

奇安信

事前可识别
- 用户识别
- 行为判断
- 内容可视

事中可管理
- 授权准入
- 应用管理
- 访问控制
- 流量优化

事后可追溯
- 事件定位
- 事件追溯
- 统计分析



上网行为管理部署在网络中，对信息合规性进行判断，实时对不当网络行为的管理

- 上网行为可视
- 防止泄密风险
- 保障合法合规
- 行为风险预警
- 提升工作效率
- 提升带宽利用率

上网行为管理ICG简介

奇安信

ICG的主要价值

上网行为可视	法律法规遵从	防止信息泄密	提升工作效率	优化带宽资源	商业智能分析
•上网人员 •访问网站 •使用应用 •传输内容 •上网时长 •上网流量	•符合82号令 •阻止色情网站 •禁止非法言论 •阻塞攻击言论 •阻止非法网站	•知识产权 •财务数据 •营销计划 •设计图纸 •单位机密	•应用阻断 •内容阻断 •时长限额 •流量限额	•限制P2P下载 •限制在线视频 •保障OA •保障邮件 •保障视频会议	•实时监控 •历史日志 •统计趋势 •智能报告

ICG功能模块

用户管理模块	网页过滤模块	应用控制模块	内容审计模块	流量管理模块	日志分析模块	共享接入模块
•身份认证 •身份识别 •终端准入 •终端识别 •位置识别	•URL分类库 •URL关键字 •网页标题 •网页内容	•应用管理 •应用告警 •时长限额 •流量限额	•网页内容 •发帖内容 •邮件内容 •IM内容 •FTP	•带宽限制 •带宽保障 •用户平均 •每用户带宽	•实时监控 •历史日志 •统计趋势 •智能报告	•防止私接 •路由器 •WIFI

上网行为管理的三个重点

奇安信

在一般的行为安全管理实践中，人们通常遵循“识别”、“管控”、“分析”的三部曲思路。而这三个步骤也都是围绕行为的三个核心。

上网行为管理的主要功能和价值

奇安信

核心价值

合规

- 法律遵从
- 企业合规：上网权限分配
- 工作效率提升
- 互联网防泄密

功能

用户识别

- 组织结构
- 用户识别
- 用户认证

内容审计

- 发帖
- 邮件
- 网页浏览
- IM
- FTP

应用控制

- 应用封堵
- 带宽管理
- 限额管理
- 每用户控制

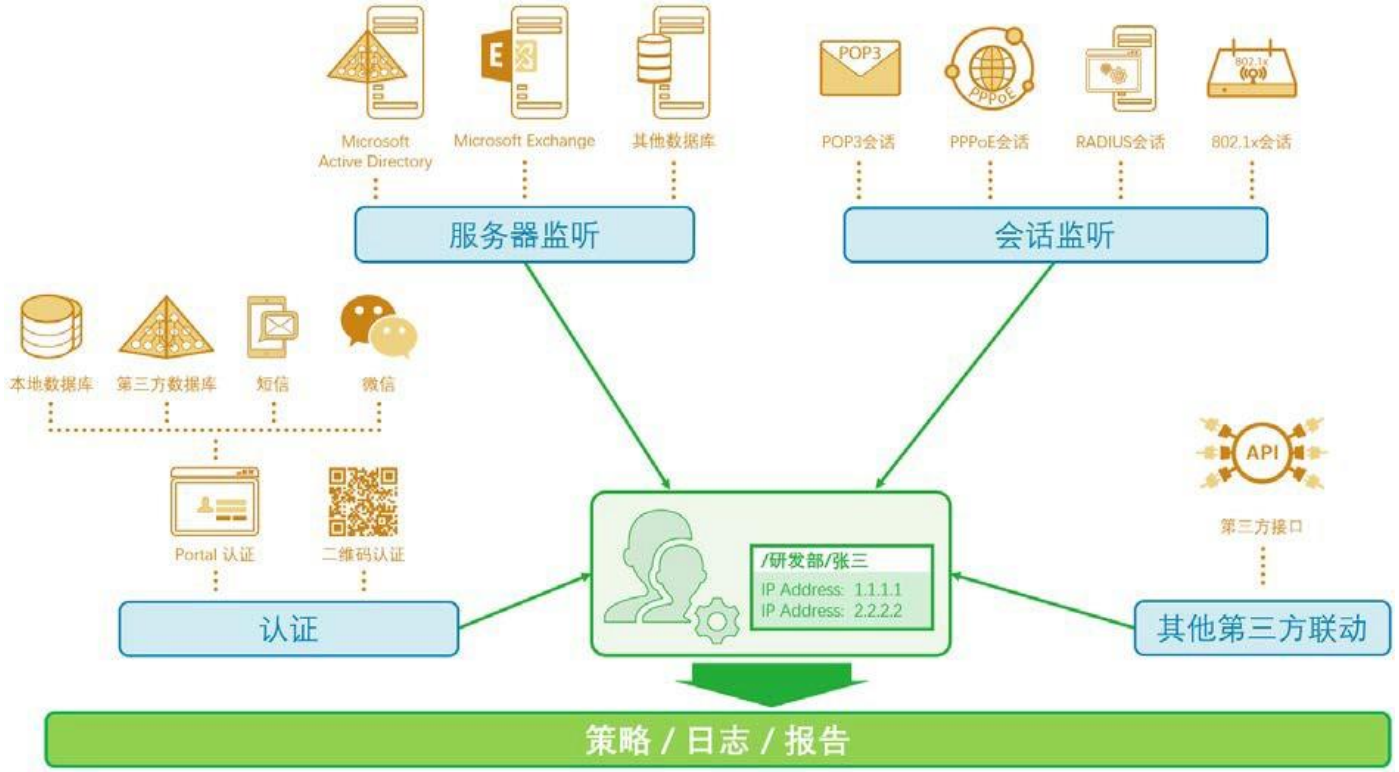
用户识别

奇安信

用户是网络行为最重要的主体，对用户的识别是行为安全管理的首要环节，也是最基本环节。没有用户识别，行为安全管理也就无从谈起。

用户识别的终极目标是为管理者提供一种使用用户名（而不是简单的 IP 地址）来创建策略、查看日志和报告的环境。

从原理角度大致可以分为四大类别：认证、服务器监听、会话监听和第三方联动。



几种认证识别方法的对比

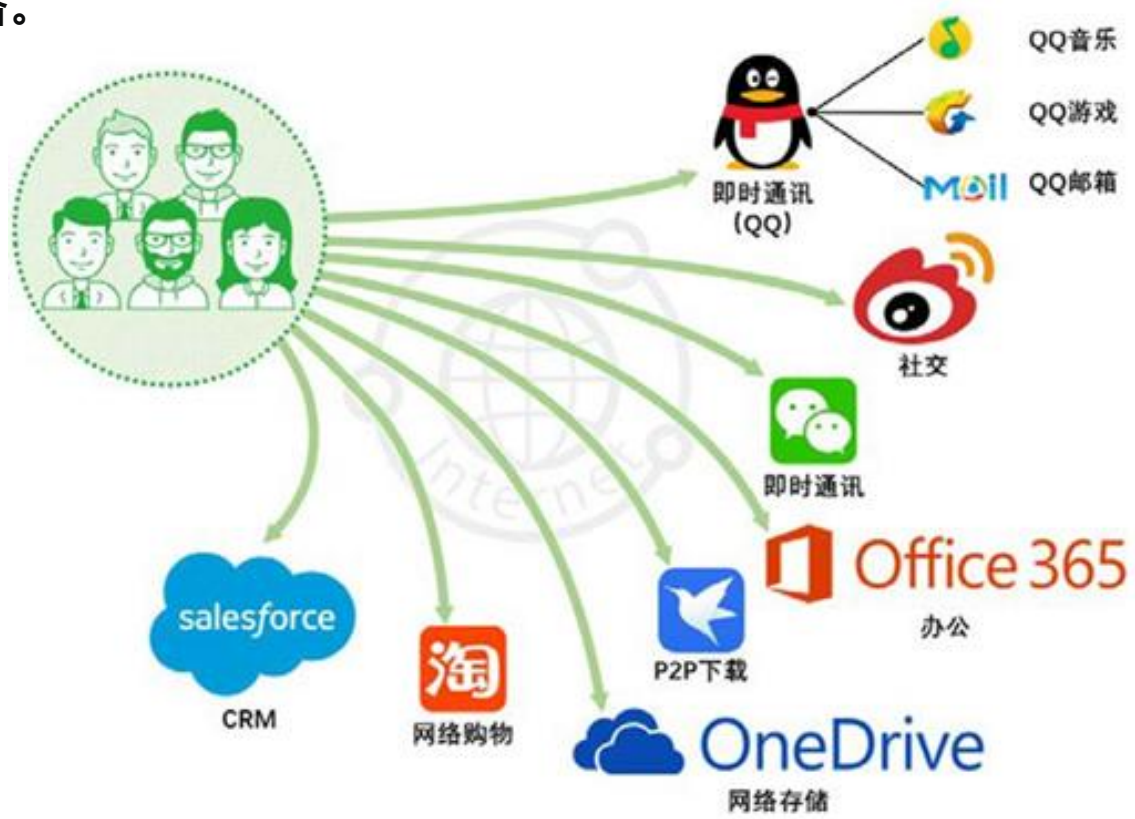
奇安信

认证识别的方式是通过用户主动提供身份信息来完成“IP-用户名”映射建立的，这些身份信息可以是用户名、手机号码、社交账号等；而监听和联动方式都不需要用户主动提供任何信息，从而实现了对于用户的“透明”，它们通过从包含有身份信息的第三方数据（如登录日志、在线用户表、网络数据包等）中直接提取或间接分析出“IP-用户名”映射关系。

方法	用户感知	识别准确率	准入能力
认证	有感知	高	有
服务器监听	无	通过外部数据获取信息，总会存在一定的未识别或误识别情况；目前大部分的用户识别模块都可以做到90%以上的识别准确率。	无；通过外部数据直接或间接获取映射关系，与用户实际产生的流量没有必然关系；因此并不能通过是否识别成功来决定流量是否可以被放行。
会话监听	无		
第三方联动	无		

应用识别

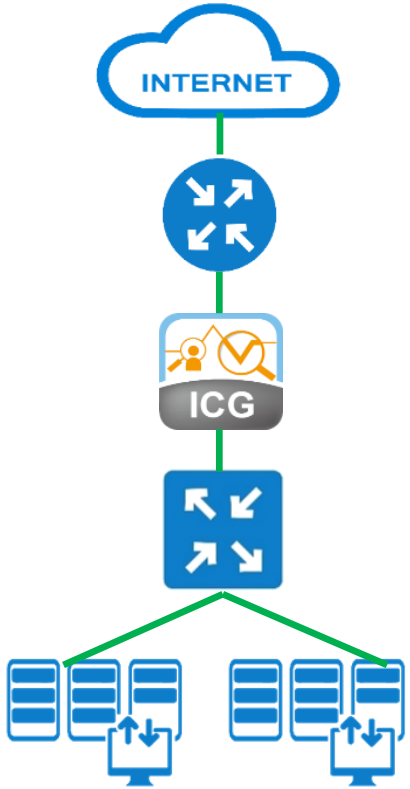
网络行为安全管理领域中所说的应用通常指特定的程序或者功能，它们的通信可以被标记、监控和控制，这些应用一般都可以产生网络流量，它们的通信方式可以是 BS 模式、CS 模式，甚至是 P2P 模式的。“标记”、“监控”和“控制”也都是行为安全管理设备针对应用所产生的网络流量进行的。网络应用是网络行为的主要客体之一，对于应用的识别也自然是行为安全管理的重要环节，应用识别的目标是能够基于应用制定行为管理策略。



设备部署模式介绍

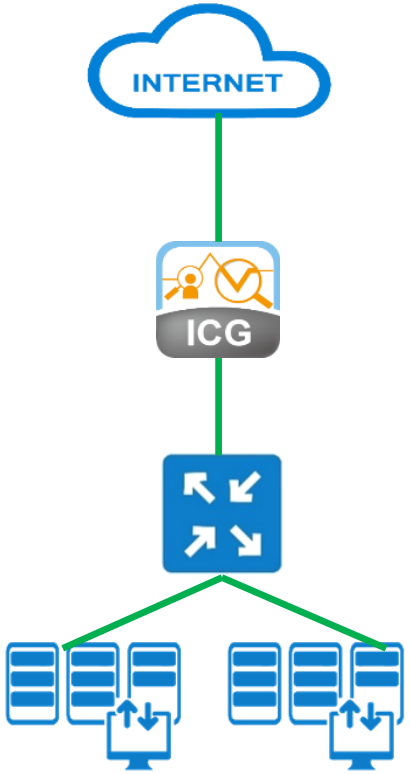
奇安信

一、透明桥接模式



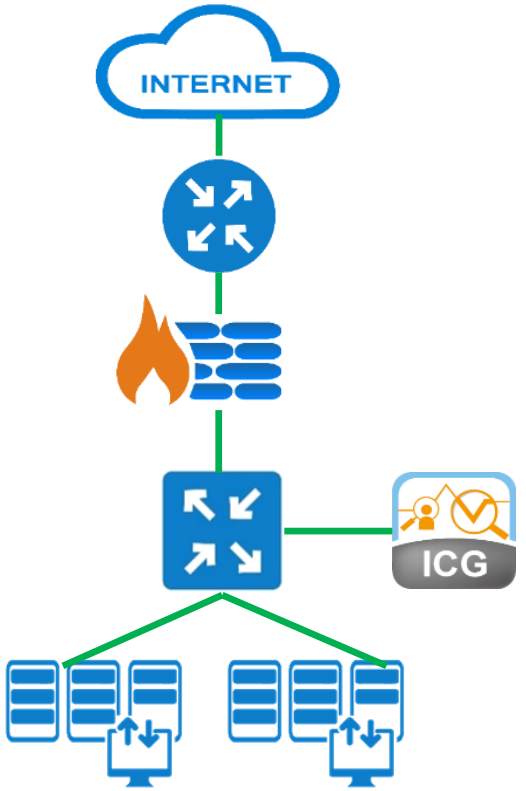
- 可识别网络中各种网络行为，并审计
- 可控制管理网络中各种网络行为

二、出口网关模式



- 可替换出口NAT设备，提供NAT功能
- 可识别网络中用户行为并审计
- 可控制管理网络中各种行为

三、旁路镜像模式



- 可识别网络中的各种网络行为并审计
- 但控制效果有限

（可对TCP应用进行Reset，UDP控制无效）

奇安信

THANKS!

让网络更安全
让世界更美好