Allot SG 快速参考手册

Contents

Allot 公司是谁?

Allot 公司是全球领先的为企业和运营商提供**网络智能化**和**安全**方案的供应商！1997 年在以色列成立，2006 年在纳斯达克（NASDAQ）上市，2010 年又在以色列特拉维夫上市，股票代码 ALLT。

Allot SG 是什么?

Allot SG 是网络智能化与安全网关， 网络智能化与业务保障平台。

Allot SG 价值定位

- 5 大功能：所有经过 Allot 产品的流量可视、可控、优化、安全和大数据分析（运维分析和运营分析）
- 关键业务优先，用户滥用防范； 网络安全保障

打个比方：SG 就像是日常生活中十字路口的**摄像头、红绿灯和交警**， 可以看到什么样的人、车通过，出现拥塞对流量进行调度和管控，当有高优先级车辆过来时，交警可以进行流量管制等， 并保障道路安全。

Allot SG 独特优势

- Allot 是业界领先的在单一硬件设备上可以同时提供可视化分析、应用策略控制和流量管理、Web 安全和抗 DDoS 一体化以保证企业业务网络最佳性能的平台
- Allot 是业界领先的可以存储所有经过设备的数据流到数据库中进行保存以便查询及进行实时 BI 分析和长期保存的平台
- 让网络更智能
    - 7 层应用的可视化； VPN 加密流量的可视化
    - 用户和终端的可视化
    - Web 内容和 Web 威胁的可视化
    - 对关键的商业应用提供更优的用户体验
- 保持网络安全
    - DDoS 保护
    - Web Security: Anti-Malware, Anti-phishing, Web filtering, 风险 Apps 控制,

Anti-DDoS, Anti-Botnet, Anti-Spam

Allot 可以帮助您解决哪些痛点?

- 网络带宽足够， 但经常性在忙时会有网络速度慢的情况，比如有时要开视频会议，影响质量； 原因不明
- 有些关键业务，运行速度不是很稳定，是否是网络的问题?
- 不知道网络中到底运行了哪些业务?

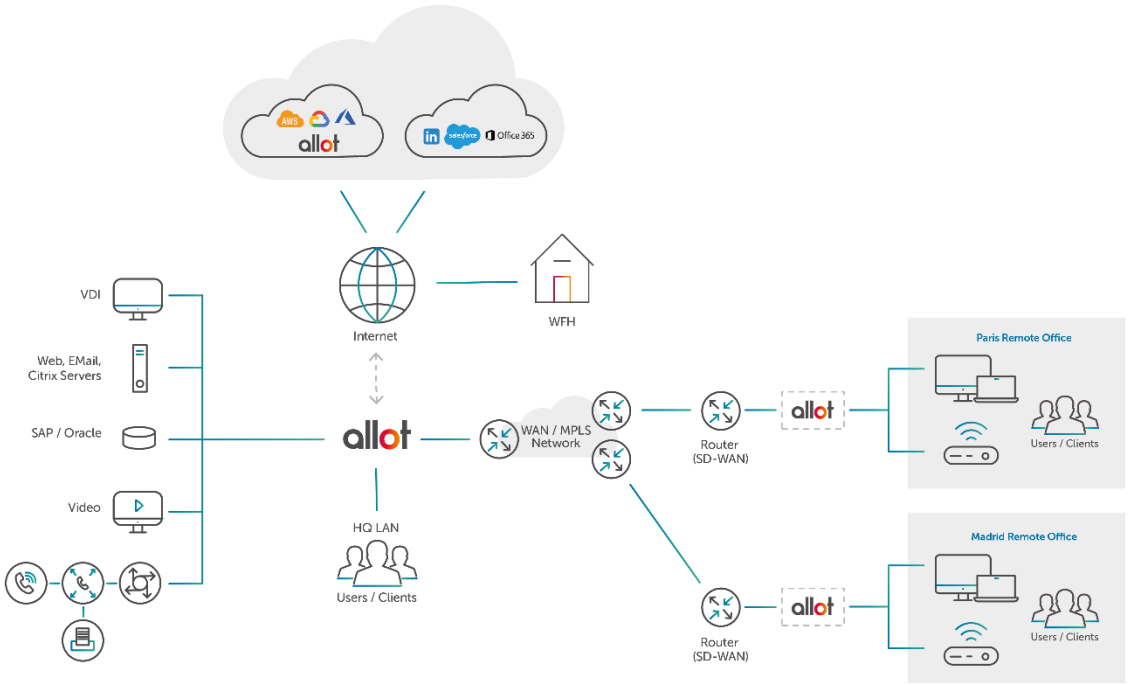
部署位置

应用在企业的 Internet, LAN、数据中心和广域网出口网络（适合于企业有多个分支机构）

部署方式

部署在企业总部和各分支机构骨干节点

示意图如下:



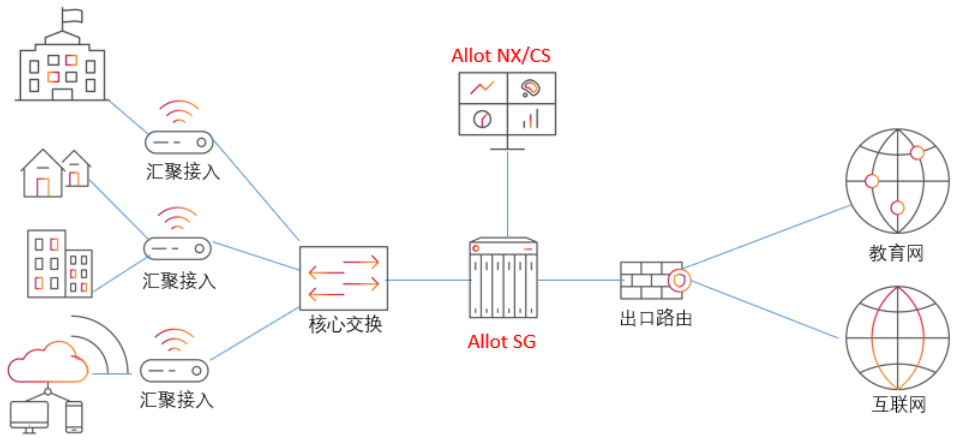
什么企业可以用到 Allot SG

- 中、大型企业 – 典型 500 – 200,000 员工
- 各分支机构需要经常访问自己私有数据中心;
- 比较少的业务运行在公有云上
- 也会经常使用公有云上的应用，比如 Office 365，视频会议等

- 业务云化比较慢 (比如：制造、教育、金融 BFSI)
- 复杂的策略管理 – 多分支机构、复杂用户类型和部门

高校应用场景

Allot 高校部署拓扑示意图



现状：

- 教职工带宽被学生占了大量带宽； 并且 P2P 在学生中是十分流行的应用： 非常占用带宽， 使学校重要的应用流量使用效果很差
- 希望控制网络流量和保持带宽预算不变
- 教育和学术研究等相关应用要优先保障
- 使用“翻墙”、加密货币“挖矿”等不允许的应用
- 图书馆电子资源使用情况管理困难，什么人浏览了什么网页，下载了什么文章不好定位，专利资源的使用情况实时反馈
- 学生使用“代理”，一个账号下挂多个终端上网，游戏和视频，不易管理。
- IPv6 设备越来越多，和 IPv4 并存
- 各种灵活、方便的流量套餐，方便选择和管理
- 区分用户的不同类别（学生、教师、管理人员、访客）
- 校园业务拥塞控制
- DDoS 检测和防范
- IoT 的智能化

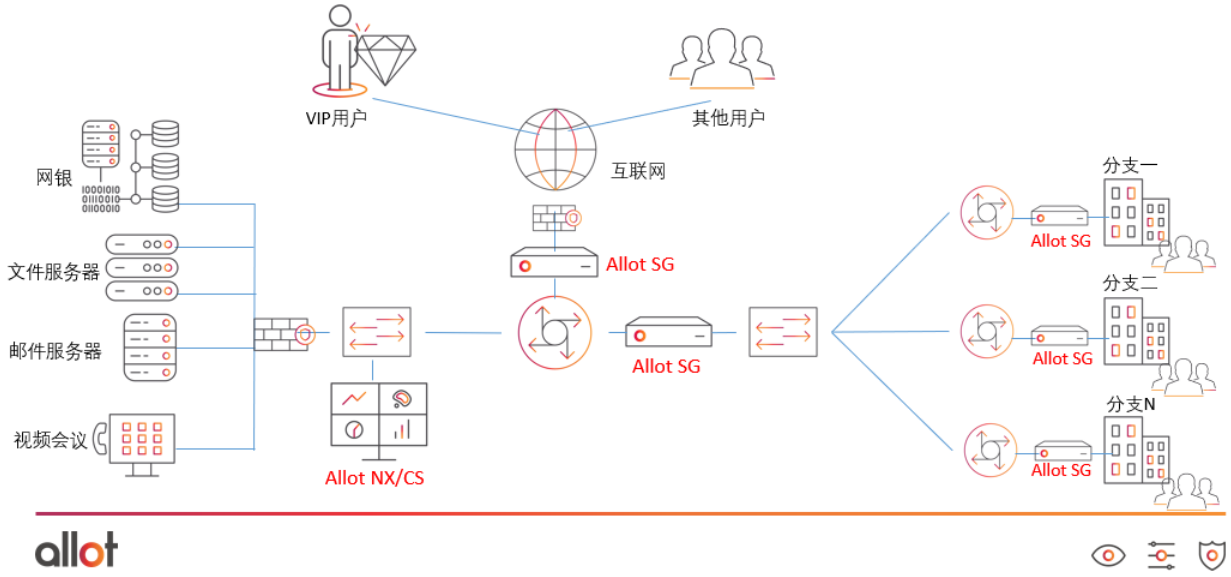
Allot 能够解决：

- 对校园内的用户、设备、应用、用户体验和安全可视化

- 控制进、出 P2P, 语音和视频流量； 各种对带宽饥渴的应用竞争网络带宽： 优先保证正常的教学和管理应用的带宽。
- 支持 IPV4 和 IPv6 的混合流量的监控和管理功能
- 对学术和管理应用的优先和动态管理控制，为关键应用保证带宽和 QoS
- 在重点保障阶段的“一键断网”功能，灵活方便
- 图书馆付费电子资源的防恶意下载； 实现查询和使用专利方面电子资源的管理，实时反馈专利研究使用情况，针对不同使用人群做到合理配置
- 与多种认证计费软件的配合，为每个用户提供流量套餐及带宽保障，对每个学生一定时期内（每学期， 上学期间）的网络访问轨迹，流量轨迹画像（比如， 上学期间使用了多少流量， 最常访问哪些网站，玩哪款游戏最长时间，学习应用占了多少比例等等）
- 对每个用户分配对应的带宽，学习、教育相关的应用带宽进行保障，并且免费。 对于娱乐性的流量免费一定流量后进行限速或做其他处理；针对不同应用计费方式/价格不同
- 流量达到配额后自动提醒缴费或者限速；跟踪和停止带宽滥用， 对某些特定应用定向免费， 最大化增加现有的带宽使用率和降低广域网的费用
- 实时 Botnet 僵尸网络检测和防范和实时 DDoS 攻击的检测与防范
- 识别、检测和按照要求管控相关“翻墙”VPN 等应用，限制“挖矿”等应用，阻断“暗网”应用
- 基于用户和基于应用级别的优先级的管理和控制
- 单台硬件平台可以支持 140G 的吞吐，完全满足学校未来几年的扩容需求
- 高密度的接口和在同一平台上支持 10G/40G/100G 管理接口
- 精细的控制颗粒度和详细交叉多层次管理规则可以应对学校复杂的监管需求
- 精细的数据监控报告以及和联动学校指定的认证系统实现基于身份的全方位跟踪
- 网络质量分析可以帮助实现定位用户访问故障

银行业的应用场景

Allot 银行部署拓扑示意图



现状:

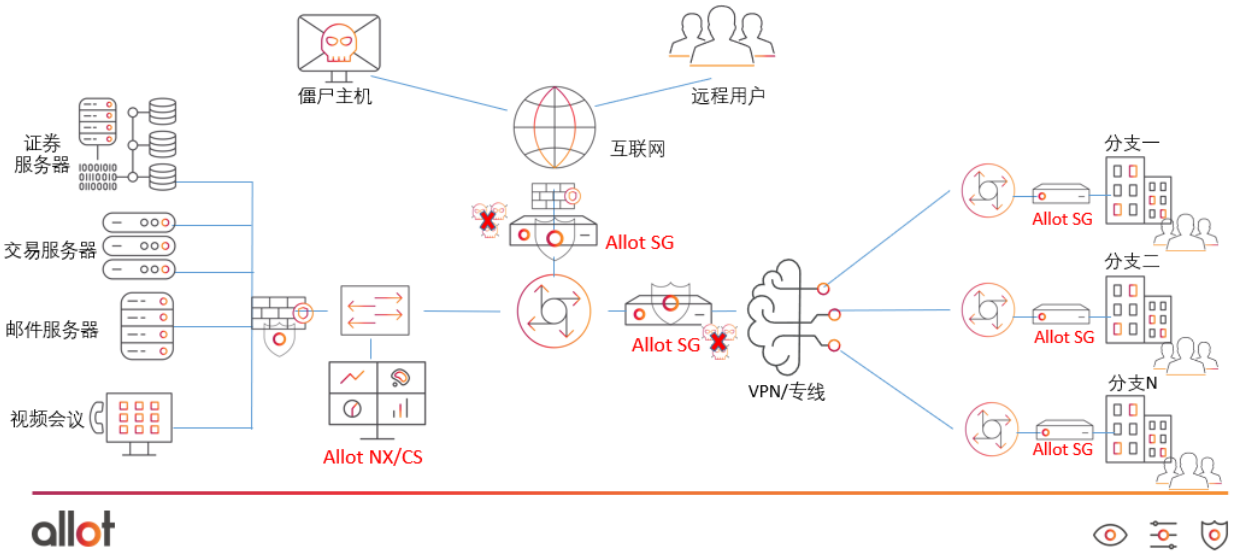
- 全国拥有多个分支行和营业网点，通过广域网分支互联
- 视频会议、邮件、ERP 系统同时并发较多（办公网络），存在带宽抢占情况
- 关键业务存在瓶颈，时常存在无法连接的状况； 在月底或者结算业务的繁忙时段，会出现拥塞的情况
- 提供网上银行服务，访问存在恶意多并发连接抢占出口带宽
- 需要对 VIP 用户、VIP 业务进行识别和保障

Allot 能够解决:

- 对银行分支单位的用户、设备以及应用行为可视化
- 对高峰期，业务系统并发抢占带宽情况进行动态调整，保障关键业务流畅访问
- 实时监控每种关键业务、关键主机的 QOE 访问质量情况
- 在出现高延时访问的情况下通过带宽优化策略来提高关键业务的访问质量
- 通过结合认证系统来实现对 VIP 用户进行识别和提高其获取的带宽资源
- 通过精细化分析系统对网上银行业务异常访问进行预警，并按照外部访问地址平均控制访问带宽

证券业的应用场景

Allot 证券部署拓扑示意图



现状:

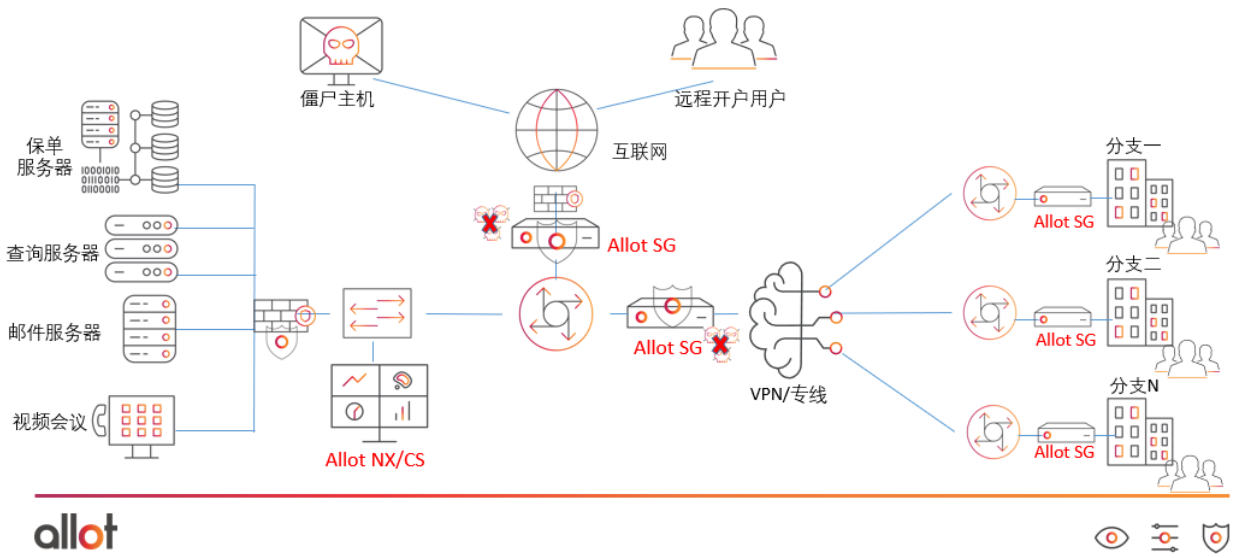
- 全国拥有多个分支公司和开户点，通过 VPN、专线连接到总部
- 分支或开户点众多，同时访问加起来的带宽远远超出总部对应出口带宽
- 需要对分支点访问的视频开会进行保障
- 多家同时访问会出现拥塞并造成大家均无法访问的情况
- 关键业务存在瓶颈，时常存在无法连接的状况
- 在数据业务出口会出现大量的 DDoS 攻击并造成防火墙瘫痪无法提供服务的情况

Allot 能够解决:

- 对证券分支单位的用户、设备以及应用行为可视化
- 对高峰期，业务系统并发抢占带宽情况进行动态调整，保障关键开户业务流畅访问
- 实时监控每种关键业务、关键应用的 QOE 访问质量情况
- 在出现高延时访问的情况下通过带宽优化策略来提高关键业务的访问质量
- 通过精细化分析系统对网上银行业务异常访问进行预警，并按照外部访问地址平均控制访问带宽
- 对业务主干出口进行 DDOS 检测，实时匹配模型并告警通知用户，并可支持和结合用户其他安全系统进行防御清洗

保险业的应用场景

Allot 保险部署拓扑示意图



现状:

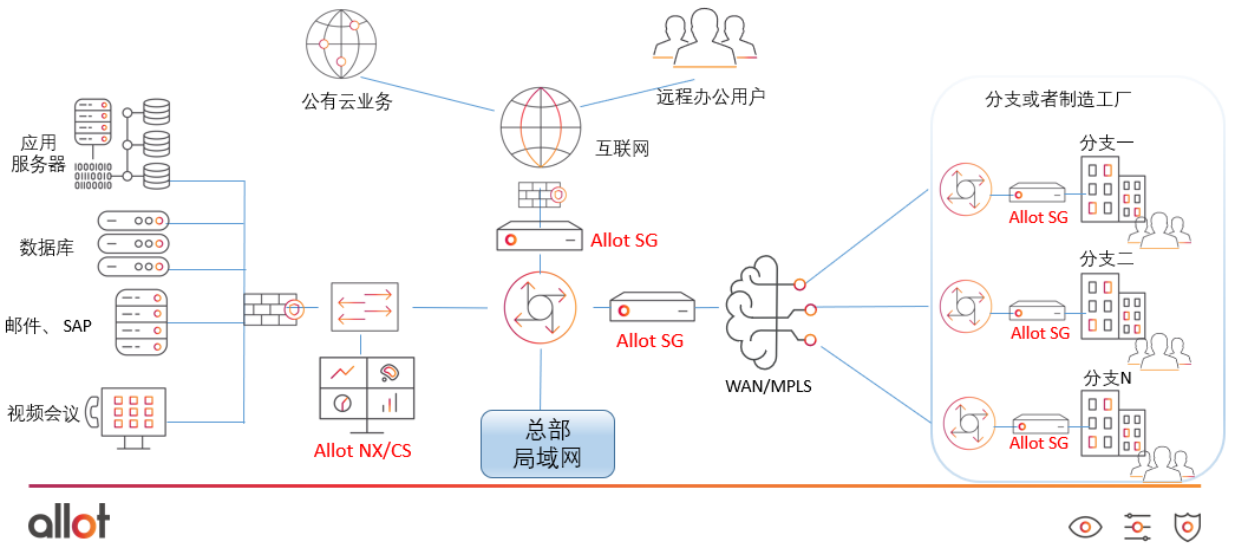
- 全国拥有多个分支或办公点
- 分支流量不大
- 关键业务存在瓶颈，时长存在无法连接的状况
- 分支业务无法精细化了解业务模型
- 僵尸网络、恶意软件和 DDoS 攻击的存在

Allot 能够解决:

- 对保险分支单位的用户、设备以及应用行为可视化
- 对分支单位的业务进行可视化管理
- 实时监控每种关键业务的 QOE 质量
- 保证和动态调节关键业务所需带宽通道
- 识别并阻断有风险的应用
- 基于网络层的病毒防护
- 实时 DDoS 检测和防范

制造业的应用场景

Allot 制造业部署拓扑示意图



现状:

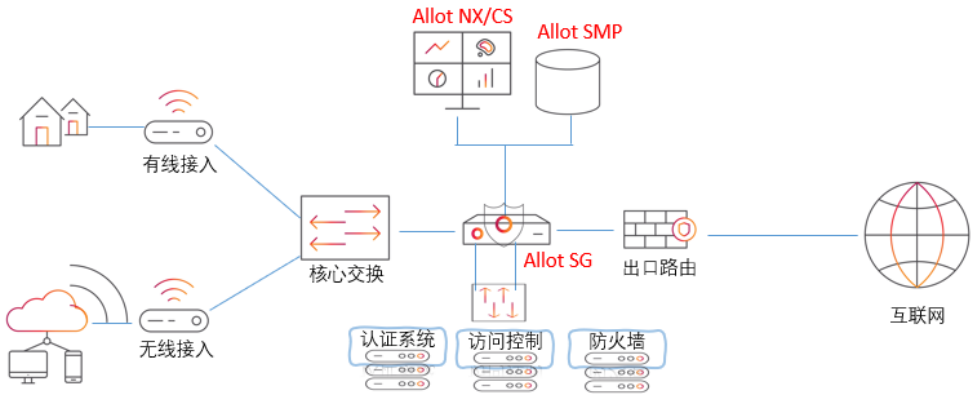
- 全国拥有基地和销售分支
- 每周都会有新测试业务和生产业务在互联网上运行
- 无法了解和控制应用对网络资源的消耗
- 不能建立用户与应用的关联模型
- 具备线上销售业务，但是存在高并发访问瓶颈
- 需要对关键业务，基于应用进智能告警
- 具备呼叫中心，需要对网络和语音数据中心进行融合管理
- 僵尸网络、恶意软件和 DDoS 攻击的存在

Allot 能够解决:

- 对基地和分支单位的用户、设备以及应用行为可视化
- 对基地和分支单位的用户、应用进行动态带宽调整和控制
- 建立用户、业务、语音的应用性能与网络环境的关联模型
- 对不同类型的业务，用户进行访问质量评估并对较差体验业务进行带宽调节
- 对线上销售的业务创建独立监控模型，并对恶意访问进行预警和管控
- 对呼叫中心的语音业务创建单独的带宽通道
- 实时 DDoS 检测和防范

酒店行业的应用场景

Allot 酒店部署拓扑示意图



现状:

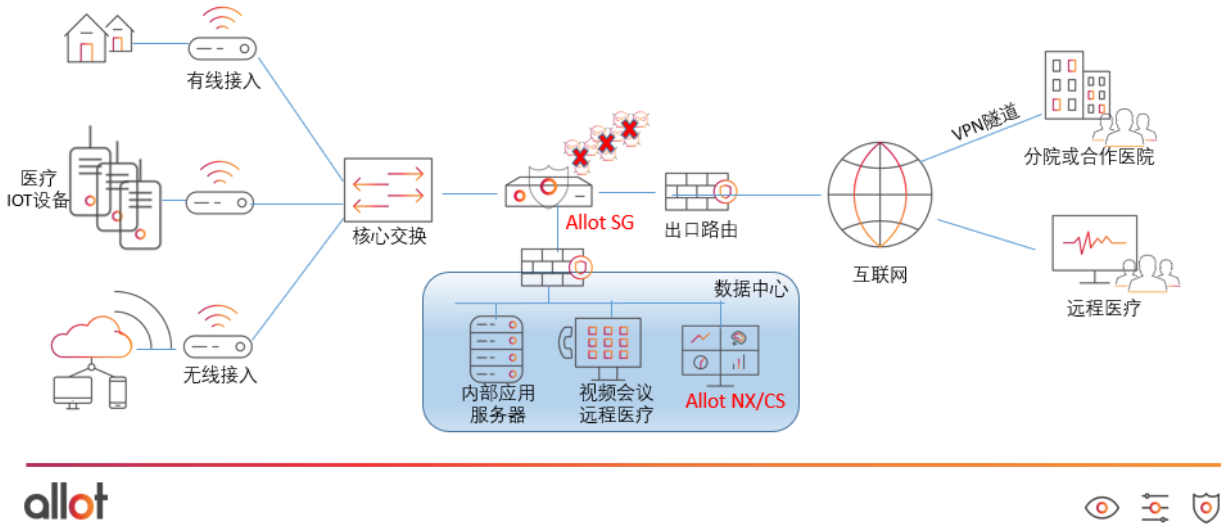
- 越来越多的使用并依赖与智能建筑等相关技术（能源、房间接入访问等等）
- IoT 增加了设备漏洞的风险
- 区分会议中心、商务中心、客房与酒店员工 Wifi 的类别
- 僵尸网络、恶意软件和 DDoS 攻击的存在

Allot 能够解决:

- 对酒店内的用户、设备以及应用行为可视化
- 识别并阻断有风险的应用
- 创建并交付不同分类的 WiFi 服务
- 基于网络层的病毒防护
- 实时僵尸网络防范
- 实时 DDoS 检测和防范

医疗行业的应用场景

Allot 医疗部署拓扑示意图



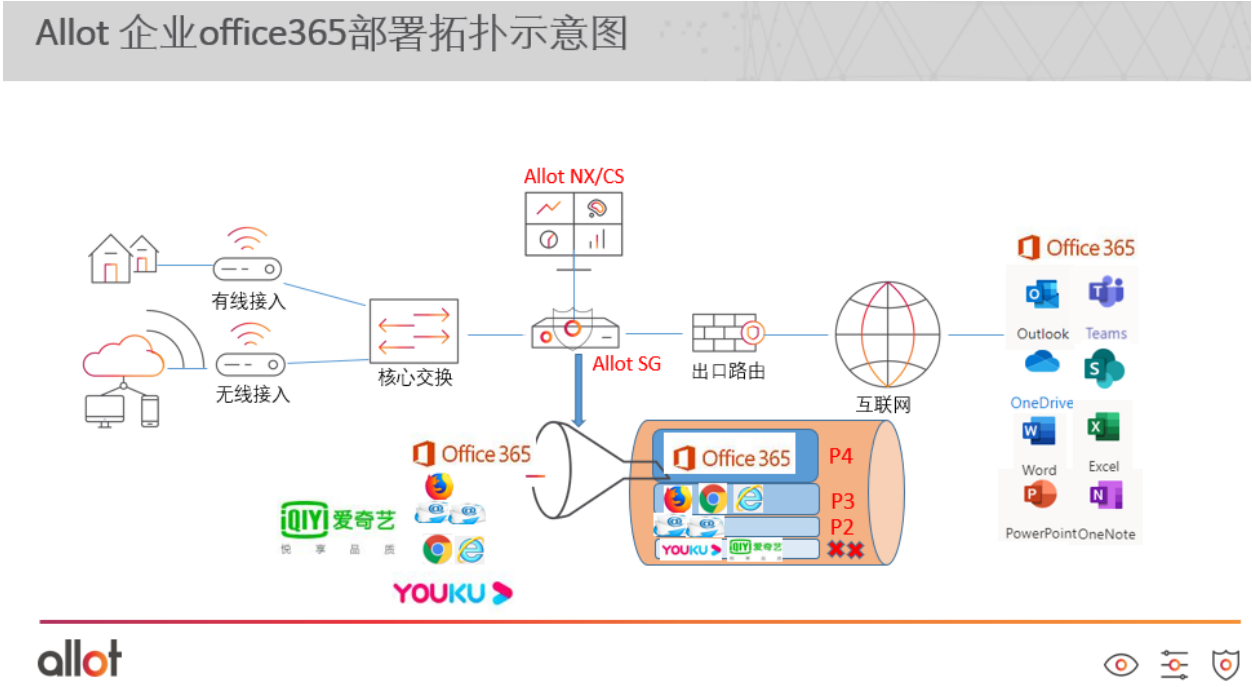
现状:

- 越来越多地使用基于网络连接的医疗设备
- 医疗设备的升级与打补丁比较复杂，对网络要求较高
- 区分不同的用户类型（病人、客人、医生和管理人员）
- 僵尸网络、恶意软件和 DDoS 攻击的存在

Allot 能够解决:

- 对医院内的用户、设备以及应用行为可视化
- 识别并阻断有风险的应用
- 创建并交付不同分类的 WiFi 服务
- 基于网络层的病毒防护
- 实时僵尸网络防范
- 实时 DDoS 检测和防范

使用 Office 365 的企业用户



现状:

- 新的应用消耗大量的带宽 (对其它关键应用造成影响)
- Lync (Skype for Business) 对实时性要求很高，视频、语音通话质量较差
- 可能出现经常性的卡顿现象（比如早上 9 点上班时大家集中收邮件时会 Outlook 卡顿）

Allot 能够解决:

- Allot 提供最好的监测和管理技术来区分 Office 365 里面不同的应用，比如 Sharepoint, Outlook, Lync 等等。
- 保障关键应用的带宽

检测和发现匿名者（ANONYMIZERS）应用需求的企业

现状:

- 企业中有加密货币等应用，占有大量公司服务器资源
- 某些员工使用未经授权的 VPN 来旁路公司的安全策略，比如通过 VPN 传送公司数据到公共网盘上
- 一般网络安全设备很难检测到 ANONYMIZERS 匿名者的应用。 比如 Tor 暗网应用

Allot 能够解决:

- 防火墙一般检测不到这种流量，Allot 以独有 的 DART 技术可以第一时间检测到这种流量

- 可以设定策略阻断或者通过告警的方式通知

Allot 超级 DPI 技术

Allot 拥有独特和领先的超级 DPI 技术 DART（Dynamic Actionable Recognition Technology），97% 的高精确识别率，0% 误判率； 可以承诺做到能够识别的流量就可以管理和控制。7 层应用识别，包括加密的协议比如 HTTPS, SPDY, Skype 和 BitTorrent； 更重要的是可以对 IPSec, SSL VPN, L2TP 等各种 VPN 加密流量的识别，对加密货币和暗网（Dark Web）应用的识别。这个也是 Allot 技术领先的地方。

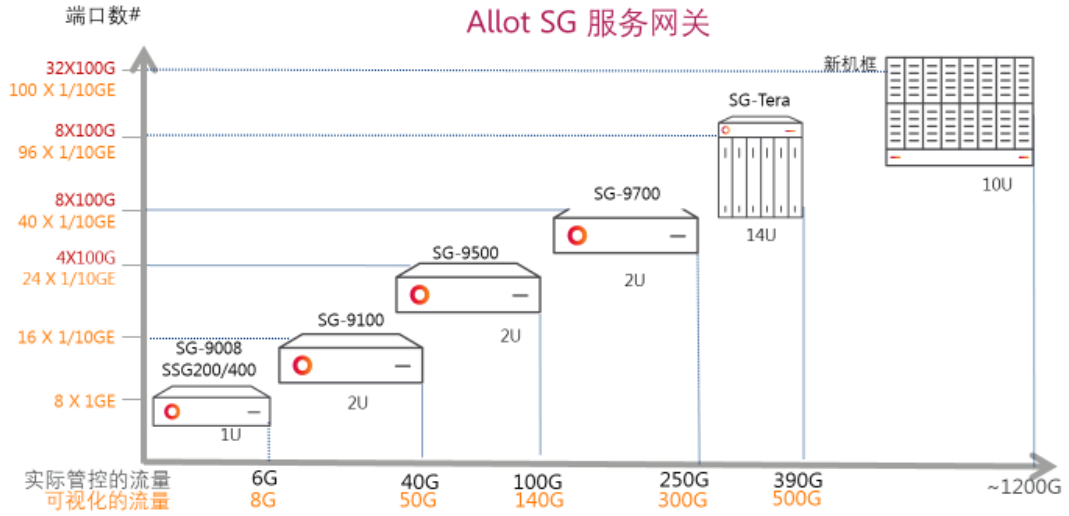
通过下面的技术对加密流量进行识别

- 模式检测
- 证书的分析
- SSL 扩展分析
- 流量启发
- 流量统计
- SNI 的检测机器学习算法
- AI 人工智能

SG 产品系列

SG Model	吞吐量	Max Connections	Max Pipes/VCs	支持员工数 (AD)
SG9700 	300 Gbps	72M (144M Flows)	512 / 4,800,000 / 9,600,000	9M
SG9500 	140 Gbps	36M (72M Flows)	512/2,400,000/ 4,800,000	4.5M
SG9100 	50 Gbps	12M (24M Flows)	512/1,000,000/ 2,000,000	1.5M
SG9008 	8Gbps	3M (6M Flows)	512/250,000/500,000	360,000

Allot 硬件平台



allot

硬件、虚拟化、NFV

硬件

S/W 直接运行在专用的标准硬件平台上

SG-9700

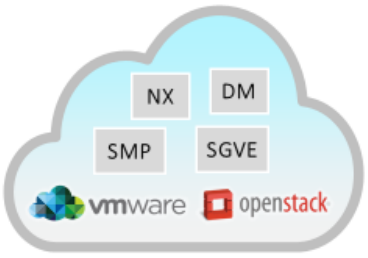
SG-9500

虚拟化

软件运行在标准硬件之上的虚拟机上面

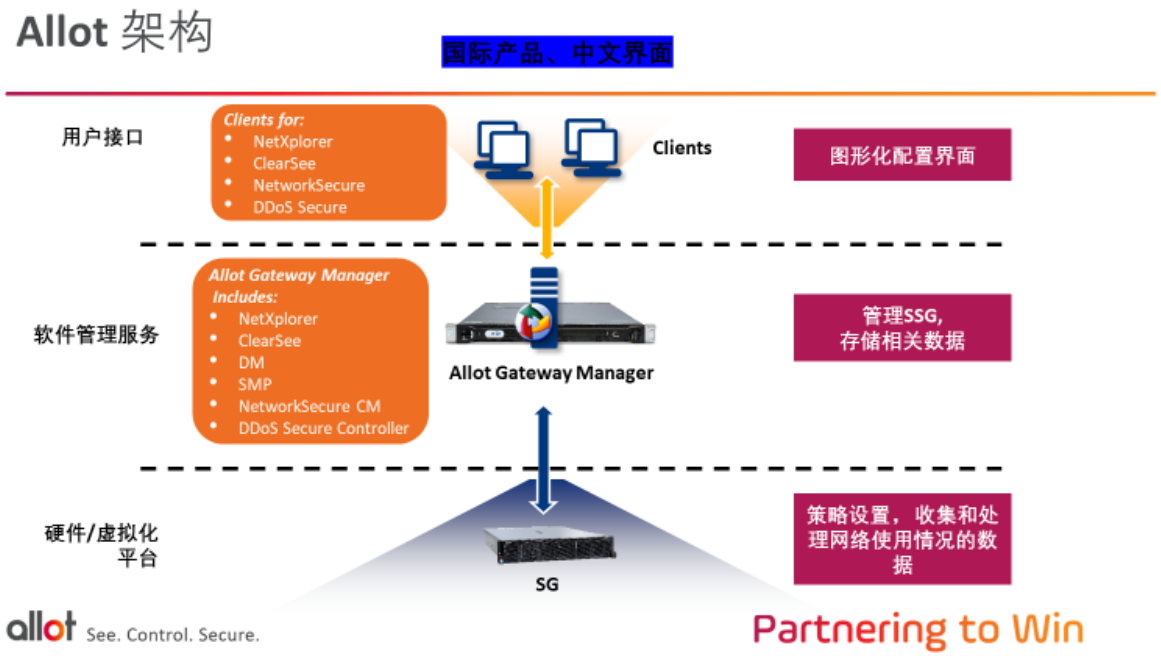
NFV/电信云

软件运行在自动化的电信云之上的虚拟机上面



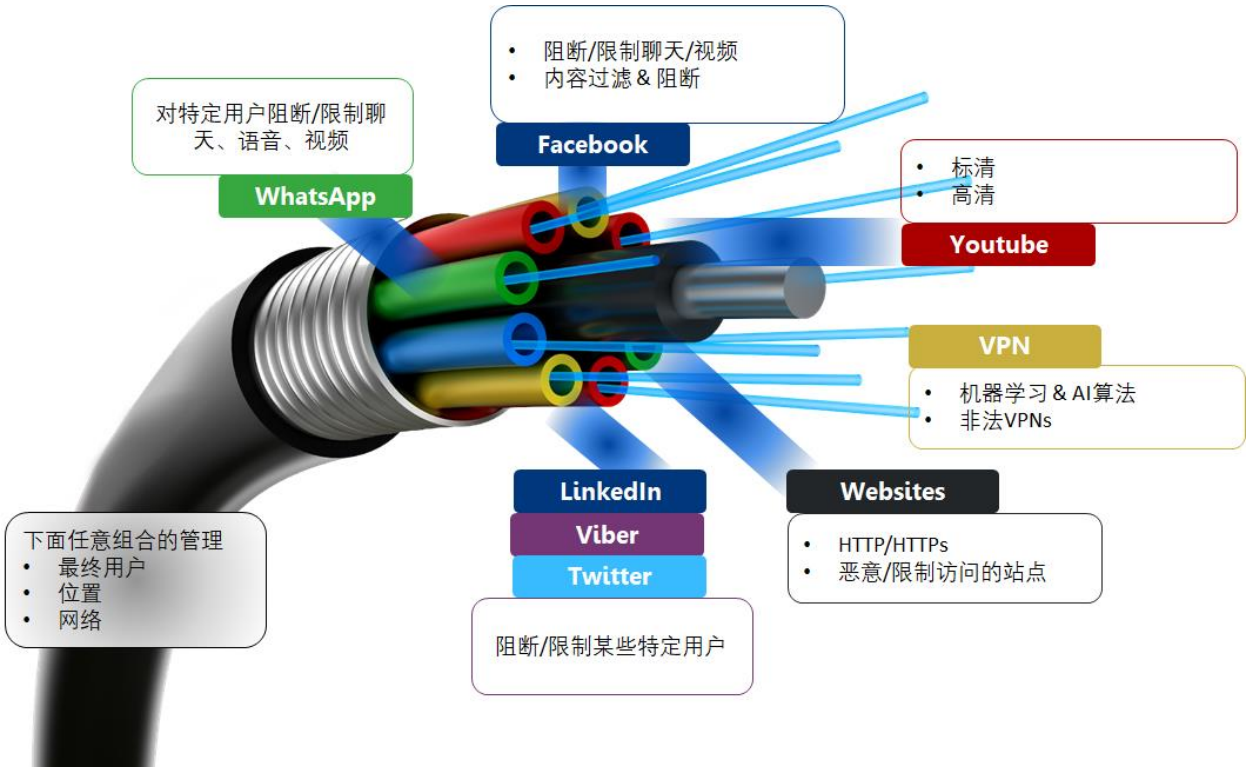
allot

SG 架构



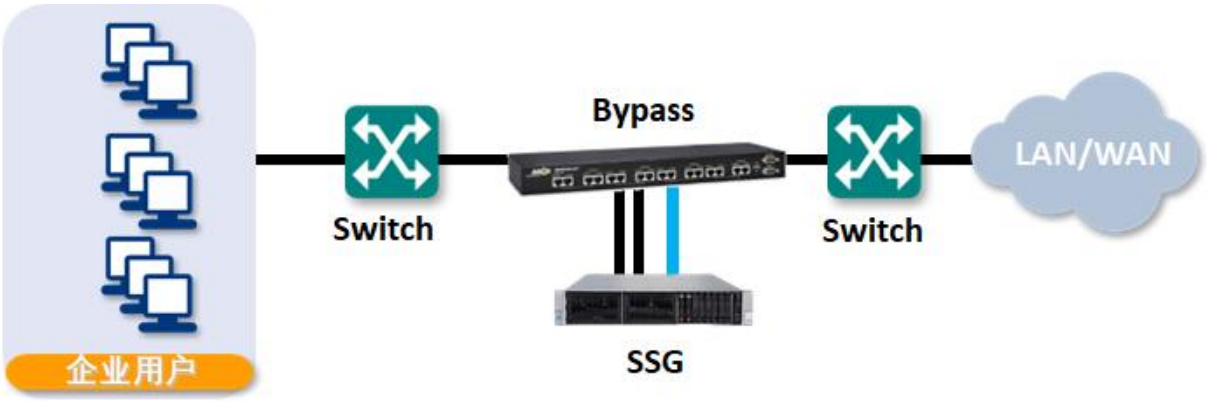
Allot 典型功能

1		可以基于位置、特定时间、对特定用户进行特定社交媒体应用的管理和控制
2		对暗网应用的完全控制，比如匿名者和公共VPN 服务等
3		基于用户的应用使用情况的实时监控 基于用户的应用使用情况的长期日志保存及智能收集分析
4		基于法律或者公司要求的内容过滤功能(WAF)
5		内、外网的DDoS防护
6		使用Man-In-The-Middle 的方法对特定用户SSL 加密内容进行安全检测和识别分析



SG 旁路单元保障业务不中断

- Allot Bypass 是一个无源旁路设备， 外接在 SG 设备上， 无需电源
- 万一 SG 出现故障或者断电，确保网络连通性，不影响业务运行， 大概 2 个毫秒就切换到 Bypass 设备上。



我已经部署了 PA 的防火墙， 是否还需要 Allot? 为什么?

产品定位不一样，PA 或其它 L7 层防火墙还是以控制访问为主，哪些能过，哪些不能，什么时候放过是它的主要核心价值，Allot 的核心价值是能过多少，谁先过，谁后过，谁能有特权，大家访问公平和提高访问效率。所以有 Allot 是为了更好的利用网络。

我有一个数据中心， 现在用了 PA 防火墙, 增加 Allot 有什么好处?

两者产品定位不同： PA 定位为 NGFW, Allot 产品定位为网络流量智能化与安全。 Allot 重点关注数据中心的性能， 可靠性、SLA, 及相关业务的 QoS.

通过 Allot 的应用分析大数据平台，可以帮助数据中心看到其内部数据访问热点，访问质量以及访问次数等情况。

现在防火墙已经有了应用的可视化， Allot 与其有什么不同?

- NGFW 提供的是比较简单的有限的管理控制（比如阻断，限速或者允许通过）和安全相关的报告。对于全流量的可视化与控制做的不够
- NGFW 有一些流控的功能， 但是开启流控功能会大大增加系统资源消耗，造成安全检测功能方面的性能快速下降
- NGFW 一般部署在网络边界位置， 对内网设备的可视性不是关注的重点
- Allot 可以对全网经过 Allot 的流量均可以可视化并实现精细的管理与控制， 特别在大型、有多个分支机构等的复杂网络情况下
- Allot 提供业务的 QoE 实时与历史分析报告，对网络运行状况实时进行分析并可预警

我已经在交换机和路由器上部署了流量的 QoS，为什么还需要 Allot? 两者 QoS 上有什么不同?

路由器和交换机配置的 QoS 层次较为单一（一般就根据端口号为某业务设置优先级， 如果 HTTP 业务与 P2P 业务均都用 TCP 端口 80 进行网络访问， 那么交换机或者路由器就无法区分这两种完全不同的业务）， 管理较为复杂。

QoS 做好后，无法形成报表展示以查看 QoS 生效情况，而且交换路由上部署 QoS 对性能会有影响，出现性能故障无法及时排除。Allot 流量管理部署后，通过详细全面的报表展现网络中出现的所有业务，以及拥塞情况。然后通过两级三层次策略集，能实现更为深入全面的流量分类和管控。

最后 Allot 的控制精确度为 1Kbps，带宽控制精确度也远远强于路由器和交换机。

几年前已经知道并且是 Allot 的用户，但有段时间没有用了， Allot 技术上有哪些更新?

Allot 技术也一直在与时俱进的更新， 主要体现在下面几个方面：

- 更高的性能以满足当前更大带宽的需求， 单台 2U 的设备可以支持超过 200Gbps 吞吐量的可视化与管控
- 支持虚拟化部署， 支持常见的 VmWare, OpenStack 平台， 部署方式更灵活
- 增加 DDoS 安全特性， 对内网的“泛洪”、外部对内部网络的攻击可以在最短时间内进行检测和清洗

- 增加大数据分析模块，增加了网络质量分析 QOE 以及用户行为画像模块，让用户更深入了解网络】
- 增加 TCP 优化/加速模块， 在网络时延较大、网络质量不是很好（比如丢包、抖动比较大的无线、卫星通信等）的情况下， 一般可以做到 40% - 100% 的性能提升
- 增加 Web 数据安全模块，可以帮助管理员对用户的网络访问进行过滤，帮助企业管理和净化用户的互联网访问

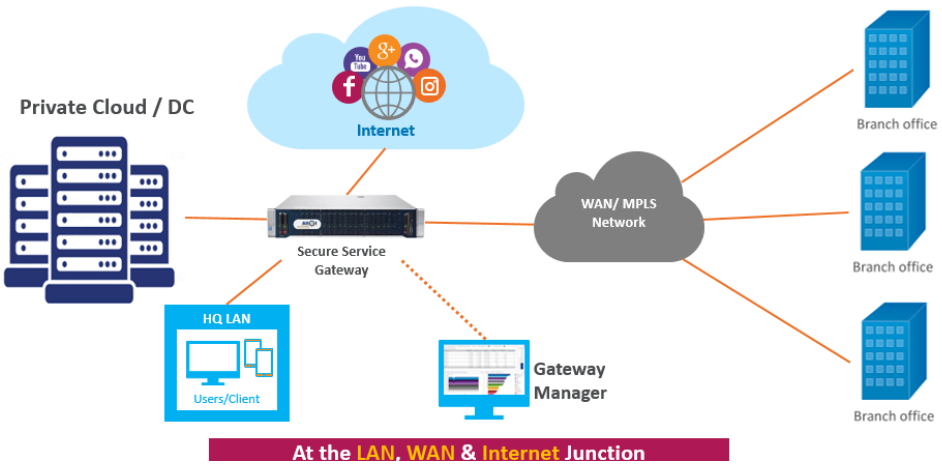
现在带宽已经很便宜了， 带宽不足，我就扩带宽， 为什么要选择 Allot 的带宽管理设备呢?

目前带宽确实比以前大很多了， 但是带宽增加并不意味着不需要管理。因为网络中的流量类别、流量也都在增大。 正像城市中的马路一直在拓宽， 但还是会经常堵车一样。

网络的智能化管理在任何时候都是需要的，这个不会因为带宽增加而消失，就好像不管拥塞与否，都会需要交警指挥交通，只是管理的方式不像原来那样简单粗暴了。在原来带宽不足的情况下，我们要做的是通过限制一些应用来达到出口不会拥塞。在新的管理方式下，管理员更多需求的是有效的调度资源，动态分配带宽，让网络资源的利用率能有效的提高。另外，通过用户行为画像，QoE 的分析，能帮助用户快速定位一些网络故障，并通过应用、用户、带宽的调节来实现一些故障的消除。

除此之外，Allot 智能管道技术可以提供新形势的自动化运维，可以随着带宽变化而改变带宽的管控。

我的带宽比较充足， 那 Allot 的典型部署位置是怎样的? 能帮我们解决什么问题?



Allot 产品采用 Inline 或镜像方式部署在企业网数据中心出口，互联网出口，广域网出口处。

- 通过 Allot 流量控制系统的智能管道技术将客户流量按照位置、业务不同细分为多组不同的

管道，并同时建立智能监控系统

- 快速不间断的业务告警
- 根据不同位置、业务建立带宽告警机制，任何异常流量突发，Allot 会根据其不同进行区分告警
- 实时而长期的监控
- 最短 15 秒一次，以及可以长达 4 天的短期报表，帮助用户可以实时掌握其业务系统的流量分布
- 用户质量分析系统
- 实时基于业务系统的 QOE 数据报告，可以生成根据不同业务系统的网络质量分析报告，Allot 可以动态生成基于 TCP 业务系统的丢包、重传、延时以及基于 web 业务的访问质量评分，极大的帮助可以看到实时的网络质量情况
- DOS/DDOS 网络安全防护
- 基于基准线的零日攻击保护技术，可以自动根据攻击流量特征来生成清洗特征库，快速清洗网络中的泛洪垃圾流量
- Web 安全访问
- Allot 支持基于 Web 业务流量的内容过滤，病毒扫描，钓鱼网站提醒重定向等多种手段，保证用户访问的 Web 业务为安全流量。该部分 Allot 支持对 HTTPs 网站进行扫描和过滤

Allot 部署，如果只在总部总节点部署一台，网络管理行不行？一般是否没有必要在分支节点都部署？

是否需要在分支部署取决于用户的流量，如果大部分资源在总部，并且从总部到分支流量较大，可以实现单边部署，只在总部部署即可，如果存在大量上传流量，存在大量 UDP 应用的流量，这种情况下必须双向部署设备。

能举例说明一下单项控制和双向控制的优劣吗？有的客户预算有限，只能上总部一台控制。

单台设备本身可以进行双向带宽管控，但是 UDP 协议本身没有确认机制，如果是存在大量 UDP 协议的应用例如备份、日志、监控，传输等从分支上传到总部，可能直接拥塞点为分支出口了，所以遇到这种情况，分支没有设备进行管控，即时在总部部署了也没有效果，因为问题本身发生在分支出口上。 因为这种情况在多数用户里面没有那么常见，所以可以一般先只在总部部署。

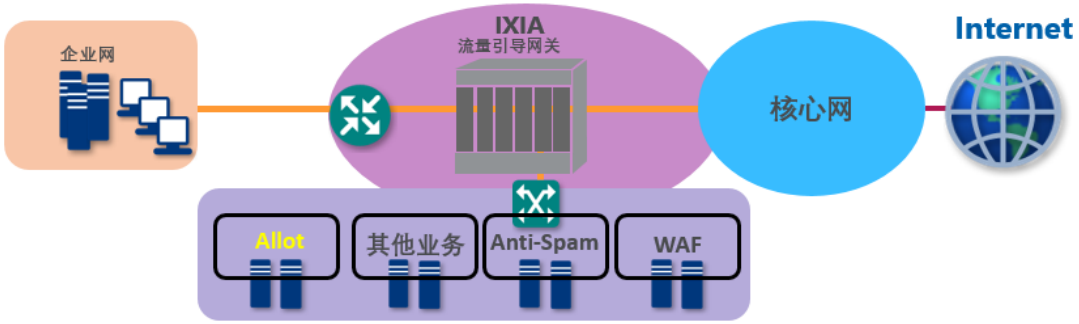
如果是关键业务系统或者较大分支，一般是需要双向都有部署和管理。

这种情况类似于高速公路的收费站，如果只是控制一个点的车流量，可能会造成高等级的车无法在另外一个城市下高速，因为另外一个城市上高速的车全部拥堵在高速口

对于平常经常需要保障的视频会议，远程电话会议，是不是 qos 优先保障会多一些？如果从总部往下发起，是不是总部流控管理就够了？

保障视频会议，远程会议是一个重要的需求点，所以会比较多，也是重要痛点的地方。从总部管控还是上下都需要部署，还是跟客户环境有关系，这个和上面的回答是一样的，主要看客户业务流向和业务类型，如果客户是典型的从总部单边获取资源那么总部部署就够了，如果存在大量 UDP 协议且上传应用比较多，建议为双向部署。

Allot 与 Ixia 一起部署图



整体特点:

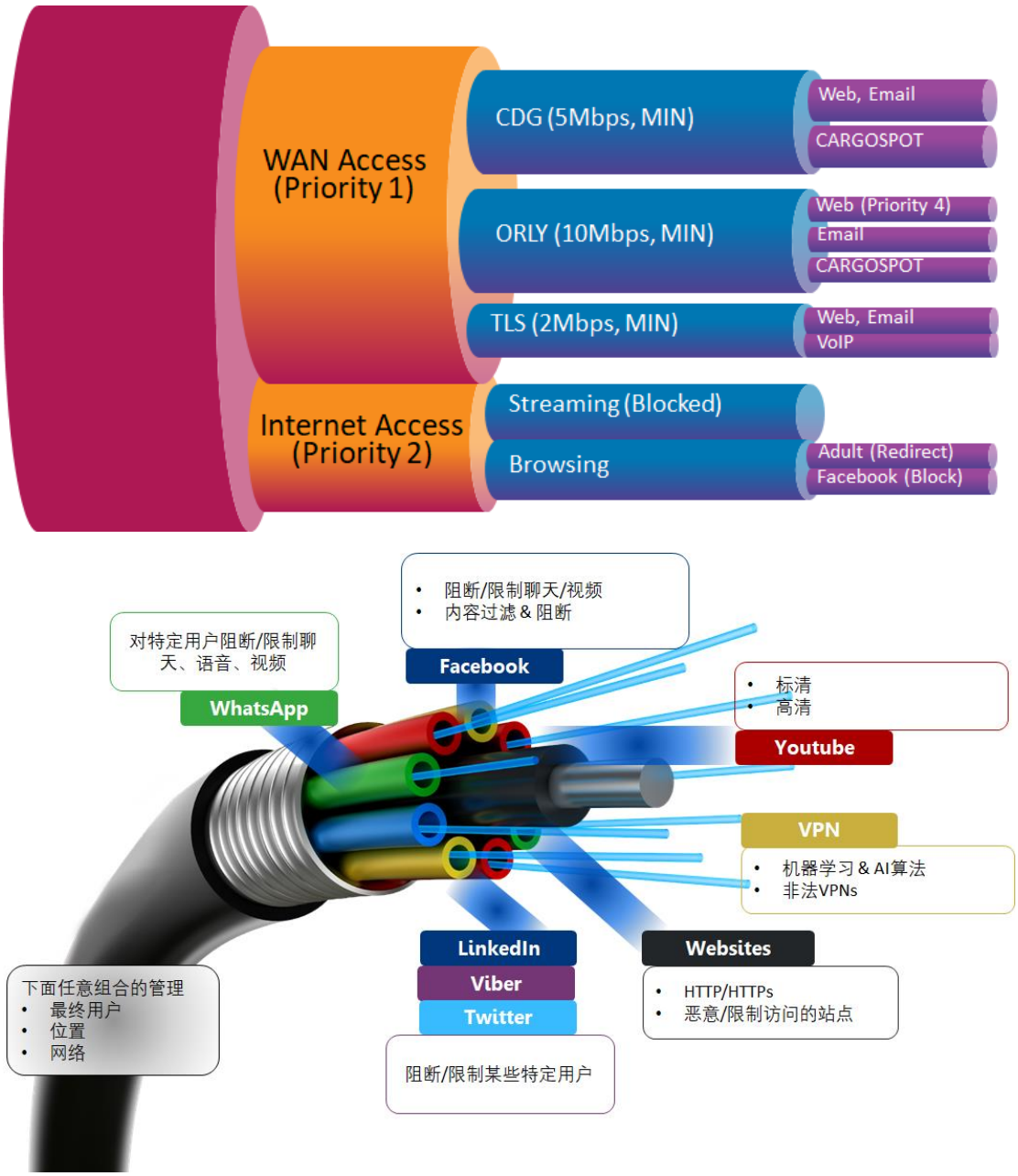
- 网络拓扑简化
- 智能化的业务应用与用户网络接入控制
- 智能化的应用与用户的负载均衡
- 降低硬件与运营成本， 仅仅重新路由相关流量方向即可
- 容易部署，最小的延时和抖动

该方案中 Allot 的特点:

- **智能流量识别、归类，生成多维度网络分析报表**
- **QoE 分析，用户、流量、七层应用访问质量分析和跟踪**
- **动态调度机制，保证流量按照应用需求获得保证带宽通道**
- **风险管控，丢弃风险应用，管理非法用户通过互联网**
- **Web 应用过滤，对病毒、木马、钓鱼网站、广告等非法应用进行管控丢弃**
- **DOS/DDOS 流量清洗, 对泛洪应用识别和丢弃，保证出口流量安全性**

Allot 是否还能针对每个用户进行流量分配?

Allot 可以对每个用户的每种应用进行流量分配和管控， 比如 A 用户同时上网， 微信， 视频，发邮件， P2P 等， 可以对每个应用根据要求进行流量分配和管控



Allot DDoS 有哪些特点？ 如何定位其 DDoS 特性？

Allot DDoS 是基于流量模型特征的解决方案，其快速响应以及自创建特征库是可以匹配所有未知的 DDoS 攻击。独有的模型分析模块，可以让用户对危险最大的破坏型攻击阻挡在发生之处。

Allot DDoS 平台定位于出口网关式流量预警清洗平台。

Allot DDoS 与竞争对手比有哪些特点？

- 超级稳定的平台， 20 多年在运营商和大型企业使用的考验

- 一个平台实现流量管理和流量清洗的全部功能
- 分类型建立流量数据模型和策略
- 快速响应并阻挡未知的流量 DDoS 攻击
- 自带攻击分析模型，定期抓包，让客户事后可以准确定位攻击特征
- 不依赖于升级特征库实现攻击的识别

Allot 与 APM / NPM 有什么不同?

Allot 侧重于出口流量 L4-L7 层应用分析，并且支持对于 TCP、HTTP、Video 特殊协议的访问质量分析。重点在出口边界质量。并且 Allot 数据分析是个长期持续报表，实时存储并支持，长期统计。

APM/NPM 侧重点在于客户端的应用、网络的故障排除和分析。用于定位应用、网络故障源点。

Allot 优势在于网络核心出口的故障长期跟踪分析，而其在需要作出优化或控制的时候可以实现出口故障排除。

APM/NPM 优势在于跟踪分析故障，但是并无法对出现故障实现消除的解决方案。

Allot 与应用审计产品有什么不同

Allot 的审计在于内容以外的数据审计，但是包括了其使用的应用以及网络 5 元组，不会去窃取用户内容数据信息。Allot 的报表还是关心网络相关数据，帮助网络管理员了解、管理其网络的需要。

审计产品更多是去跟踪用户的内容信息，包括，聊天信息，关键字搜寻等。主要是满足用户对国家特有审查的需求。

所以两者在设计上存在明显的不同。

Allot 与竞争对手相比有什么特点?

- 硬件稳定：Allot 的产品定位电信运营商级别。产品覆盖最新多核 X86 和机架式 NP 架构，产品经过长期运营商运行测试
- Allot 性能参数均为开启全部功能情况下，且企业级提供 100G 线速，运营商 500G 的单台硬件平台
- 对于用户控制精确度上，可以轻松的创建以人为单位，以应用为套餐的精细化控制策略，

  同时开源的数据仓库可以帮助用户实时结合其他日志分析系统来实现数据的联动分析

Allot 的导流功能和 Tap 交换机有什么不同?

- Allot 重点还是流量管理的功能， 流量重定向后，还能识别协议控制带宽，还可以出报表， 以负载均衡探测，可以基于应用重定向