格物资讯
Gawain Research

电子政务外网的今天与明天

——访大连市政府网站管理中心主任耿昭

2013.3

目录

电子政务外网主要服务于各级党委、人大、政府、政协、法院和检察院等部门，是为各部门业务应用提供网络承载服务的重要基础设施。经过十多年的规划建设，我国已建成连接各省、市及中央各部委的电子政务外网骨干，正在向区、县乃至街道、乡镇延伸，以便更好地满足各级政务部门进行社会管理、公共服务的需要。

中办 18 号文件下发后，建设统一的电子政务网络平台成为我国政务信息化建设的主导思想，推动着各个业务系统的互联互通与资源共享。而在国家电子政务外网二期规划中，数据中心与共享灾备、统一的运维与管理等新技术、新运营模式也被提上了建设日程。它们能否顺利落地？业务应用是否藉此变得更高效、更灵活？资源整合对运维造成多大难度？政务信息化程度的加深又会带来哪些新的安全隐患？带着诸多疑问，格物资讯走访了大连市政府网站管理中心，与耿昭主任进行了几番深入交流。

大连电子政务外网建设情况简介

作为我国政务信息化起步较早的城市，大连很早就开始整合信息资源，探索合理的电子政务建设方式。早在 2002 年，大连市就推出了城市门户网站“中国大连”，公众以此为入口，可以联系到社保、税务、工商、公安、交通车辆管理等政府办事机构。

经过一年多的摸索，大连市政府网站管理中心于 2004 年正式成立，以统一建设、统一运维的方式为各政务部门提供网站服务，确定了构建统一的硬件支撑平台建设与应用的整体规划。中办 17 号文件下发后，该中心又被赋予了建设并管理全市集中统一的政务外网网络基础平台、应用支撑平台和安全支撑平台的任务；同时，面向政府内部业务部门的大连市政府数据中心也开始建设，逐步承载起一些纵向专网业务系统的运行。

2008 年 12 月，大连市政府网站管理中心完成了“大连市电子政务外网统一平台示范工程项目”的建设工作，提供了包括网络管理、安全防护、容灾备份等技术服务功能于一体的政务外网统一平台。该平台目前承载着网上报税、网上社保、公务考录等 700 多个应用系统，被国家发改委作为示范工程列入高技术产业发展项目计划。

走向大型化、无线化的基础网络

网络基础架构是电子政务外网的承载体，直接决定了业务实现的形式与体验。大连的经验表明，由已知需求主导的有线网络升级改造是大势所趋，接入向街道与社区的延伸使更多基层部门具备了实现政务信息化的手段。另一方面是由点到面的变化，WLAN、3G/4G 等无线接入技术的成熟普及让业务形态变得更加灵活，为电子政务外网的未来发展与应用描绘出极具想象力的空间。

格物资讯：在拜访您之前，我们在网上看到不少大连电子政务外网建设方面的信息，但大多比较陈旧。关于目前外网建设和应用的情况，还请您先简单介绍下。

耿昭：大连市电子政务外网统一平台的网络基础架构是基于全交换实现的，这和地域条件有关。因为大连本身地域不是很大，节点之间的距离不太远，全交换的网络足以支撑。从目前承载应用的情况看，性能也没有出现瓶颈。用户接入方面，目前光纤通达所有区县和街道。不过政府扁平化建设有着三级体系的目标，未来可能很多政务工作都会放到社区一级去做，所以目前我们正在做 1600 多个社区的接入，一些大的社区也采用了光纤接入，个别偏远地区会用 ADSL。

格物资讯：在统一出口方面目前是什么样的情况？未来又有哪些规划呢？

耿昭：按照要求，目前大连市电子政务外网的 3.2 万个用户都通过统一出口访问互联网，所有网站和业务系统也通过这个统一出口进行发布，便于管理并且安全可控。在接入上我们有两个原则，第一是应接必接，一定保证在目前中国通信体制下做到就近接入。第二是多线冗余，一旦哪条线路出问题，其他接口还能保证业务畅通。目前统一平台上有上百个关键性的业务，比如报税这种，是一秒钟都不能停的。所以我们现在用链路负载均衡设备接了一条 1G 的联通出口、一条 1G 的电信出口和 1G 的教育网出口，让一般的互联网访问只走联通和电信，同时确保就近接入的原则。服务器区的负载均衡设备也启用了智能 DNS，保证给外网访问者返回最快的接入地址。下一步我们在考虑接移动的链路，主要是为了移动手机和移动 WLAN 用户的接入。

格物资讯：您刚提到了手机和无线接入，目前这样的接入需求很强烈么？

耿昭：这是一个趋势，毕竟无线覆盖可以满足移动需求，让接入变得更灵活。我们现在基于 3G 的业务很多，比如计生委就在用平板电脑做人口入户普查。未来 4G 的应用可能会更广泛，除了通过运营商接入，我们也会在达沃斯会展中心等大型活动区域和政务密集区域有自己的 4G 接入点。

格物资讯：您的意思是自行建设 4G 网络，而非租用运营商的资源？

耿昭：会有一部分是我们自己的，业务要逐步架构在组合型方案上。我们已经做过一些测试，感觉 4G 接入总体上是稳定的，同时它的性能和灵活性可以支撑更复杂的业务，比如应急指挥、移动视频会议和移动的视频监控等等。

格物资讯：会有很多业务用到 4G 移动终端么？

耿昭：从成本角度考虑，大部分政务用户在一段时间内还是依靠 3G 或 WLAN 实现无线接入。我们更多地把 4G 当做骨干传输，落地还要靠 WLAN 这种成熟并且低成本的方式。这可能是一个主流方向，比如大连周边的一些海岛，目前光纤已经拉过去了，但在岛上铺光纤要受到很多环境上的限制，成本也比较高。用 4G 覆盖就方便得多了，我们测算了一下，很多岛用一个基站就能满足所有单位的接入需求。

从“做加法”的管理者到“做减法”的运营商

顾名思义，应用支撑平台是以业务为核心，保障其正常运行的技术实施手段。但业务迁移速度远远落后于基础设施建设速度，是现今电子政务外网普遍存在的问题。对此，大连的做法是两手抓、两手都要硬，在业务与硬件方面坚持“做加法”的同时“做减法”，真正贯彻了电子政务外网取代化、集约化的建设精神。

另一方面，如今业务与支撑平台的耦合度越来越强，企业 CIO 已经开始更多地介入业务环节，成为决策团队中的重要角色。政务信息化领域也是如此，随着应用支撑平台所承载业务的增加，相关部门也不能再以管理者自居，要用新的思路、新的方式更积极主动地建设、运营电子政务外网，在减少自身压力的同时提高统一平台的稳定性与可靠性，保证行政与服务的需要。

格物资讯：在网络区域划分方面，大连电子政务外网是如何规划的？

耿昭：按照要求还是规划了互联网、内联网、数据交换和横向互访 4 个类型的区域，承载的业务比较多，像 VoIP、视频会议也都利用数据交换区建立了单独的子区域。横向互访区现在业务量很大，我们的目标是用它和内联网区把政府目前涉及到的面向社会公众的业务全部承载起来。运营上目前分成网站管理中心和政府数据中心，二者间有万兆链路连接，做到实时备份。有些资源根据服务对象的不同是两边都有的，比如人口、法人单位、宏观经济、空间地理和自然资源库等等。

格物资讯：很多地区的电子政务外网还是个“胖网络、瘦业务”的情况，但我们了解到大连将原有业务往统一平台迁移的进度非常快。这是怎么做到的呢？

耿昭：在“做加法”的同时“做减法”是很重要的，如果建了统一平台却没承载什么业务，或者只运营新的业务系统，那就是重复浪费。大连一直都很重视“做减法”，我们明确了替代原有专网系统的目标，通过政务外网承载绝大多数的业务。这肯定需要一个过程，所以我们会和相关单位协商一个期限，比如在几年内把业务逐步切换到这边。

格物资讯：您提到的“做减法”确实非常重要，除了业务上“做减法”，物理上是不是也有类似的要求？

耿昭：基础网络建设方面就不必说了，计算和存储资源也不可能是简单集中起来，还需要统一规划，用先进的技术方案去降低成本和运维复杂度。比如我们从 08 年开始做服务器虚拟化，到现在算是做得差不多了。这其实就是一个“做减法”的过程：我们最早机房里面是一千多台服务器，上了虚拟化以后减了几百台，这几年逐渐又把老旧服务器换成稍微高端点的型号，总数量一直在减。

格物资讯：虚拟化的概念很热，但对于很多用户来说也存在是否能落地、对业务产生价值的问题。在您看来虚拟化都带来了哪些好处呢？

耿昭：第一是资源的最大化利用，刚才说了服务器数量一直在减少，做完虚拟化后大多数系统的资源占用率在 50%以上。第二是资源分配非常灵活，比如我们监测到虽然有 50%以上的网站流量很小、负载很低，但也有一些业务系统的资源需求很大，并且负载一直在增加，我们必须不断地给这样的应用分配更多的资源。第三是更安全，之前我们用虚拟主机把很多负载较小的网站放在一起，安全性难以保证；现在一个网站一台虚拟机，安全和管理的问题解决了很多。另外还有一些运维上的需求，虚拟化可能是唯一的解决方案，比如按照我们业务增长的速度，如果不用虚拟化，不建统一的数据中心，光电费就承受不了，管理人手也不够用。

格物资讯：刚才您介绍的时候我们有种感觉，您及所带团队的工作思路不是去做管理，而是去运营一张网络和一个平台？这有点像大企业的路数，和运营商、高校或者 IDC 的场景都不完全一样。

耿昭：实际上我们就是政府的运营商，贴近业务去做网络和 IDC 的建设运营，这是大势所趋。我们现在还在做一个大概三千千伏、五千到八千平米的新云计算中心，建成后大连市所有政府部门的信息化支撑实体都集中过来，各个局不必再自己运维。运营的思路其实是在这些年逐步集中化的过程中产生的，几十台服务器承载的业务可以管理，上千台服务器（编者注：即虚拟机）就没法管理了，逼得我们必须去运营。

格物资讯：运营理念到底是什么呢？

耿昭：主要还是集中资源，专注去做核心层面的工作。我们现在团队有十几个人，规模不算小，但人力绝对谈不上富裕，所以像基础设施运维这种劳动密集型的工作是外包出去的；数据中心的运维管理、安全保障和标前测试等与业务紧密相关的工作，我们还是坚持自己去做。这里说自己做是不看过程

看效果的，比如系统加固，我们大概有 20%左右的系统用 Windows 平台，基本都是其他单位直接托管过来的，这块我们用浪潮的商用加固产品来做；其他主机一律运行 Linux，系统加固都自己动手做，这样节省成本并且更安全。我对团队的要求就是一定要保证精兵强将，每个人都得能独当一面。当然不可能什么事上来就都会做，那就组织学习培养，最后人员能力强了，工作自然就变得简单了。

格物资讯：有些工作即便整个团队一起做也不那么容易吧，比如基础架构升级之类的大工程？

耿昭：那种特殊时期他们都快累死了。比如说千兆升万兆，换一台设备就要重复一遍配置导入导出和策略优化的工作，看着几千条策略才能知道我们真的有那么多的业务，厂商的人也很清楚。日常运维的话还好些，像服务器的配置策略、安全策略和日常运维管理变更策略已经实现了一体化，准确来说现在就是一个人完成这些工作。这个人平常还做我们云终端和其他虚拟化平台的测试工作，水平是比较高的。包括他在内的小团队还曾经尝试对一些云终端产品进行过二次开发，目的是在移动终端上能对我们的业务有更好的支持。

格物资讯：您刚才提到的这些工作，我们感觉有一些已经属于厂商或者集成商实施的范畴了。您认为这也是运营的一部分么？

耿昭：有些事情我们是一定要自己做的，这是原则问题。就好比我们要用一个碗，它不带把手，端起来烫手，我们有能力给它粘一个把手，让它有用并且好用。我们只会去做粘把手这个事情，永远也不会自己做碗，因为不管人力还是专业化能力都不够，专业的事情还是要留给厂商去做。但只能粘个把手并不意味着我们完全不知道做碗的方法，我们的人员是要具备很多专业知识的。比如在做虚拟化之前，我们用了两个多月的时间，把当时市面上主流的虚拟化平台全部测试了一遍。通过实地部署几个应用，一来考察产品性能和可靠性，二来也看我们是否能把虚拟化平台运转起来，也就是和业务要求、运维要求综合起来考虑。发现问题我们会和厂商交流，这个时候做为用户就必须了解技术和发展趋势。实际证明有些厂商过来大包大揽说它产品啥都支持，测试过、沟通过以后才发现很多我们要用到的特性在未来版本里才能实现。

UTM/NGFW 的第二春？

在大连电子政务外网中，UTM/NGFW 已经逐渐取代传统防火墙，成为更细粒度安全策略的执行者。但它们的部署思路与传统概念中有很大不同，皆因运营者在安全保障方面有自己一套完善的方法论，UTM/NGFW 仅作为落地载体的一部分，不能从系统中独立出来。这样的做法会不会是个例，尚无法判断。不过考虑到大连电子政务外网的示范效应，未来也许会有越来越多的用户借鉴这种思路，UTM/NGFW 也可能翻开行业化应用的崭新篇章。

格物资讯：之前我们了解大连电子政务外网建设情况时看到，你们的基础网络建好后一直没有过大的升级，而安全产品无论从种类还是数量上都一直在增加，甚至还部署了深信服的 NGAF 这种多功能整合型产品。一般越是大型用户越愿意采用专品专用的部署思路，大连反其道而行之的原因是什么？

耿昭：你看到的是一种表象，实际上这个问题很复杂。我从事信息安全工作多年，认为信息系统的安全防护工作一定要从底层干起，比如从链路层往上一层一层剥，剥得干干净净。如果用防火墙，必须用异构部署，就是用不同厂商的产品进行多层防护。另外要把策略拆分，形成立体防护，也就是说多台防火墙上不能配同样的策略，一定是交叉着写。这么做能减小被渗透的几率，攻击者即使突破一层防护，也难形成完整的攻击行为。

格物资讯：这也是现在大连电子政务外网的安全防护思路？

耿昭：大体上是这样，但在深度和广度上要找到平衡，毕竟我们业务种类太多。业务种类多意味着运维管理和安全防护的复杂化，因为可重复的工作少了。现在在 4 层上，我们还是去把策略拆分做立体防护，有些在物理交换机实现，有些在虚拟交换机实现，有些在防火墙实现。这两年引入带应用识别控制功能的设备，主要用在 7 层流量的控制上。比如数据中心里一个对外发布的网站，从虚拟机到网络边缘做了全程的 4 层访问控制策略，现在已不足以保证安全合规，因为一些木马甚至 QQ 在这种情况下仍然是可以对外通信的。而有了 NGAF 这样的设备，我们就可以在 7 层上做更精细化的控制了，现在的要求是每台服务器或者每个业务对外的应用协议是固定的，这就是我们用 NGAF 来做的事。像刚才说的服务器，如果出现 HTTP 以外的流量，那

就可以判定为异常了，我们要配策略去进一步限制。4 层控制和 7 层控制之间没有取代关系，它们组合成细粒度更高的立体防护体系，才能保证更高的安全性。

格物资讯：您说得非常有道理，现在很多国外企业机构都采用了 7 层协议白名单制的控制思路，甚至有些行业规范里也出现了类似要求。但如果只是为了 7 层协议的识别和控制，为何不用专业流控产品实现呢？

耿昭：这个问题是要综合考虑的，受财力和人力限制，我们不可能购买、运维那么多同类型不同厂商的专用产品，也不愿意网络效率变低、拓扑变得更复杂。所以希望每种安全业务至少有两类以上的设备可以实现，彼此间有个互补的作用。比如刚才说的 4 层访问控制，交换机可以做，防火墙也能做。这样一来能做到立体化防护，二来提高了可靠性。也就是说一旦其中一个设备宕掉了，另一个设备还能把业务担起来。有一种情况是我们经常遇到的，就是设备升级反而造成了误识别、误报或者误防。我们第一时间的处理方法肯定是把相应功能关掉，因为底线是不能影响正常业务。但系统也不能因此就裸奔，此时就需要上下游的设备临时顶上，开启同样的功能、加载同样的安全策略。这下就有了足够的缓冲时间，再慢慢和厂商沟通、解决问题。

格物资讯：也就是说你们要保证这些构建立体防御体系的产品在功能、性能上都要有充分的冗余？

耿昭：可以这样理解。我们在标前测试阶段就会很严格地去考察产品，带策略的和不带策略的、实验环境中的和真实环境中的、开启单功能和多功能的情况都得心里有数，一般光测试就得半年以上的时间，到真正上线可能要两三年。上线以后会把功能逐渐分出去，有可能一台设备就专品专用了，比如你看到的用 NGAF 只做应用流量的识别控制。如果遇到宕机，第一步就是把出问题的设备拿掉，互补设备先顶上。这个时候因为开了其它功能，可能它 CPU 占用率从 20%蹦到 60%，但不会影响业务和安全性。顶过这一阵，等故障设备的问题解决了，再回到 20%的常态。现在我们考察设备，都会明确告诉厂商主从关系，也就是每台设备平时做什么、一旦出了问题的时候还要做什么，厂商也逐渐接受了这个理念了。

安全之所倚：分层、立体化、联动

除了运维，保证电子政务外网的安全是大连市政府网站管理中心最重要的工作。一个有着 3.2 万用户、承载着 700 多种业务和数十个纵向专网、同时满足互联网访问和公共服务发布需求的复杂网络，其安全需求绝不是上几台设备就能解决的。基于多年工作经验和对业务的理解，耿主任提出了分层、立体化与联动的方法论，明确了目前及未来安全防护工作的方向。同时，对于应用流量失控可能对业务可靠性造成的影响，运营者也没有一味地去打压流量，而是借助缓存设备为用户提供了更好的应用体验。这种以用户为本、变堵为疏的成功经验，值得所有网络运营者借鉴。

格物资讯：除了更精细化的控制，大连电子政务外网在涉及到公众服务的区域还用到哪些安全防护手段？

耿昭：安全防护体系的规模比较大，实现也比较复杂，我们的核心思想就是在各个环节做立体化、精细化的控制，这比单纯上一堆安全设备防护由外而内的攻击更有效。刚才说了 Web 服务器到出口，其实后端的数据库到 Web 服务器也有类似的访问控制策略。除了 IP、端口这种 4 层控制，还有单独的设备去做审计和应用流量管理，只允许数据库协议的流量通过。

格物资讯：你们的访问控制策略就做到 7 层协议为止么？是否会基于应用协议信令做控制？比如 HTTP 只允许 GET 这样的控制？否则如果成功运行起一个 WebShell，岂不是可以规避刚才提到的所有防护手段了？

耿昭：这种是有的，但是不会在安全设备里做。安全设备上做的策略一定是相对通用的，越个性的越要在终端上面做。实际上如果把 WebShell 跑起来，说明终端至少一部分权限被获取了，本地策略也可能被修改了。安全设备封住一次，攻击者可以换一种手段再试，还是治标不治本。所以立体防御体系中还有一个重要的环节就是主机端，我们是基于 Windows 和 Linux 都做了强制访问控制，规定每个账号有权利使用哪些文件，允许读、写还是其它操作，以及能够访问的进程。因为我们大部分都是 Web 服务器，你就算进来可能也没有意义，因为所有的文件都只能看不能修改，也传不了任何东西。你想传个脚本上来运行，对不起，这些都是禁止操作的。

格物资讯：现在入侵的目的更多是获取数据，对于数据库又有哪些防护手段呢？

耿昭：数据库服务器是没有外网 IP 的，想接触必须通过前段的 Web 主机。我们在数据库这块还有增强型安全机制，禁止了很多操作。攻击者对数据库表项或账号做任何操作，我们都会收到报警。总体来说你可以认为我每道关卡都不是很高端很强大，但你必须突破所有关卡才能做成一些事情，成本和难度都是很高的。

格物资讯：听起来已经比较完善了，但这也只是由外而内的正常访问流程。如果有电子政务外网内部的用户，不管主动还是被动，进行了带有恶意目的的操作，又如何防护呢？

耿昭：电子政务外网的区域规划原则就是不能互访的，内网用户如果访问内部资源就不能访问互联网，访问互联网就不能访问内部资源，这样可以规避掉实时的受控或基于跳板的操作。如果是间接的数据窃取，比如通过木马记录下访问的内部资源，等连通外网时再发送这种，我们主要靠两种方法去限制。第一是互联网区的上网行为管理设备，会有一些策略去限制已知木马的行为；第二是我们旁路部署了一套网络威协识别产品，通过模式识别去检测木马的行为。两个产品配合起来用，发现问题就实时跟踪、告警。对木马光用技术手段是没用的，管理必须得跟上，该断就断，该通报就通报，才能让所有用户都重视。几年前我们发通报都是一堆感染主机，每台都能报几百次安全事件，只能弄个 TOP 排名，到现在慢慢才算是清理得比较干净了。当然没有告警不代表就没有木马了，安全防护永远不是做了就一定安全，只能说不做就一定不安全。

格物资讯：相信净化内网的过程肯定不像您讲的这么云淡风轻，在这个过程中，你们遇到哪些困难，又是如何解决的呢？

耿昭：一开始的时候我们每天都下日报，包括安全日报、威胁日报等等，督促各级部门进行排查。后来人家也有点糊涂，因为他自己看不到网络里的情况，没有技术手段发现问题、解决问题。所以我们做了一件事：现在不仅是出口有上网行为管理，在绝大多数大型接入区也都部署了二级上网行为管理设备。这一样有两个好处，第一个好处是他有了自己排查问题的手段，分摊了我们中心的压力；第二个好处是他自己可以管理自己，包括应用流量控制也好、安全策略也好，在不违背我们集中管理策略的原则下自己优化调整。

格物资讯：上网行为管理也不只用到安全功能吧？像政务外网这种服务器与上网终端共用一套互联网出口的结构，不管你出口带宽有多大，不做流控也肯定会影响关键业务，造成安全事件。

耿昭：在互联网区的流量控制是分级做的，总出口的设备会做一些粗粒度的带宽保证，不会去看流量具体是什么应用，协议识别控制是下面的设备去做的。你说的带宽问题其实我们也有感触，未来电子政务外网要接更多的用户进来，总不能说建了统一平台就把用户体验搞下降了。所以在增加带宽和做流量整形的同时，我们一直在找提高带宽利用率的方法。前年我们部署了一台大型的缓存设备，它有一些机制去把比较热门的资源抓取下来，现在看基本上能让我们节省 20%-30%的带宽资源。

格物资讯：刚才聊了这么多，我们觉得您除了对业务理解得很深刻外，对安全技术和产品也很了解，不妨也谈谈您在这方面的看法。

耿昭：其实安全方面的考虑一定是要从业务需求出发的，比如我们为什么要对应用流量做识别控制，很重要的一个原因是很多 7 层协议管道化了，不继续剥是不行的。也有些产品技术不能满足现在的需求了，比如网闸。这个东西我们是需要的，但它效率一直上不去，没法满足业务增长，像网上报税这样的关键业务最后只能把网闸都撤下来了，现在也就是四大库这种业务量和实时性要求不太高的地方还在用。还有一个就是 IPS 和 IDS 基于非特征模式的阻断，我们现在也不建议采取透明方式去做，因为误判的可能性和代价都是很高的。有些业务系统在逻辑上类似木马或者远程控制，你给断掉肯定不行。我这么说不代表不看好基于行为的识别，相反我非常看重，但是第一是目前真能做到很好效果的产品不多，第二就是即便有很好的效果也要慎重去配严格的策略。

格物资讯：确实现在基于单体设备发现问题的有效性已经很低了，很多安全事件必须综合不同设备的检测结果才能做出判断。我们最近测试下一代防火墙的时候就有个感受，在用户身份统一后，它实际上已经具备了结合多种安全业务做关联分析的可能，去挖掘更多的隐藏威胁并做出智能响应。

耿昭：我个人认为未来的安全设备发展趋势应该是多设备联动，当然多个模块也算。更安全只是一方面追求，完整目的准确说来还是保障业务需求，涉及面很大。比如防火墙发现一些问题流量来了，除了做防护，还要会告诉链路负载均衡和上网行为管理说，把第一套策略换成第二套策略。当然这个整网策略我必须提前做好预案，但不一定要写死。理想状态是能让用户定一些

原则，比如哪些关键业务是绝对不能断的、哪些流量是平时要保障但非常时期可以断的、哪些安全业务的检测力度是非常时期要加强的，然后根据具体情况去浮动。这一系列工作现在是用户自己把控的，我希望未来在设备层面能有一定的智能化实现。

格物资讯：设备层面的智能联动不是没有厂商提过，但要不产品方案走向私有化，要不就是开放协议却很难形成健全的生态系统。您愿意被特定厂商绑死吗？

耿昭：我明白你的意思，开放与否实际上不是个技术问题。就现在我们和一些厂商交流的情况看，用开放标准实现多设备联动应该会有不错的方案。其实原来我们做 SOC 实现安全管理的联动效果就还可以，但它是纯粹基于安全这条主线来做的。现在我只是希望能在此基础上再进一步，不仅仅是做安全方面的集中管理和联动，还能做到应用交付层面的集中管理和联动，应该是有可能的。

用终端虚拟化保障业务安全

近段时间与行业用户交流，听到最多的抱怨就是终端安全无法保障。这次耿主任说的一句话就很有代表性：手机平板都能接入了，难道还寄希望于终端安全？但终端安全的问题又无法回避，如果云到端的业务链条上出现一个安全缺口，最终面临的很可能是千里之堤溃于蚁穴的残酷局面。

在经过多种尝试后，大连最终确定了终端虚拟化这种与众不同的解决思路：既然无法保证终端安全，就全力保证业务安全。不过终端虚拟化的部署也要面临很多困难，有技术层面的，也有非技术层面的。期待大连的试点工作能顺利开展，将成功经验分享给更多用户。

格物资讯：现在移动办公是个大趋势，很多情况下网络边缘已经模糊了。比如您刚才提到计生委用平板电脑做入户普查，还有权限比较高的用户可能随时登陆网站或者业务系统的后台，这个时候又如何保证安全？

耿昭：其实这么多年搞安全总结下来，数据大集中也好，移动办公也好，都让终端越来越简单，也越来越不安全。手机平板都能接入了，难道还寄希望于终端安全嘛？保护核心数据和访问通路的安全才是重点。所以除了服务器的系统安全和数据安全，我们现在要求所有访问都通过设立的 VPN 区域来接入，目前使用的是数字证书加密码的 SSL VPN 进行统一的安全认证，这样除了隧道安全外还可以对所有的用户做身份识别，在策略分发上统一了。

格物资讯：这个 VPN 区域在管理上用到什么特别的手段么？或者说，为何选择 SSL VPN，而不是常见的 VPE？

耿昭：VPN 接入的用户在权限策略和审计策略方面都是很严格的，包括我们要求任何的策略调整、信息维护都必须走 VPN 区，因为只有在这里可以做到基于特定业务、特定权限的精细控制。另外 VPN 区域的业务流量不大，可以做到行为和内容的精确审计，包括每个用户的每次登陆、修改过的策略、上传的内容都会记录。这样谁干了什么事情都是清清楚楚的，出了问题能定位到人。IPSec VPN 在权限上没法做到这么细，易用性方面也比 SSL VPN 弱一些。

格物资讯：不管是移动办公还是远程维护，终端上的数据又如何保证安全

呢？

耿昭：刚才说过，保证核心数据和访问通路的安全已经有很成熟的解决方案；终端上现在不是不想控，是控制难度太大，才造成完整业务链条末端出现了一个安全真空。其实按照现有成熟的理论模型，如果业务系统本身在数据签名、数据加密和数据保护三方面都比较完善，即便没有 VPN 也能保证一定的安全性。但是我们不可能要求几百个业务系统都达到这种程度，所以才会去做系统加固、去建 VPN，把很多安全防护工作先做了，再慢慢去促进解决业务系统在终端运行的安全问题。

格物资讯：这个问题似乎已经不局限于移动场景了，所有电子政务外网用户其实都存在终端安全的问题。那么大的用户量肯定没法去做审计和细粒度的权限控制，数据安全也没法保证，比如插个 U 盘就能把数据带走。对此，您解决问题的思路是什么？

耿昭：理论上终端安全我们可以通过上网行为管理去做准入控制，如果客户端病毒库不够新或者补丁不全，就拒绝访问。但实际操作中我们没有这样做，主要不是技术上的问题，而是管理层面的问题。数据安全确实很麻烦，受制约的因素就更多了，比如基层用户的安全意识就是个很大的问题。对于这两个问题我们希望找到更好的解决方案，也测试过很多产品，目前比较认可的就是终端虚拟化的方式。这种方式其实是换了个思路，对我们来说更现实。不管终端上有病毒也好木马也好，甚至用网吧的电脑登录上来，都不会把安全威胁带到电子政务外网里。

格物资讯：终端虚拟化确实可以很好解决问题，但是目前成本太高。而且您刚才提到有些地区的网络接入条件有限，是不是也会影响使用体验？

耿昭：是的，所以我们在终端虚拟化上有云终端和虚拟桌面两种思路。刚才你说的就是云终端，所有工作放到云端来做，也就是我们的数据中心；电脑和网络只是用户登陆的管道，并且这个管道是加密的，传输的也不是实际数据。虚拟桌面就是类似沙盒的思路，用终端本地的计算、存储资源，部署门槛就低得多了，而且我们可以把策略做细，比如不开虚拟桌面也可以访问互联网，但不能登陆税务系统。

格物资讯：您更倾向于使用哪种方案呢？

耿昭：现在只能说终端虚拟化的大方向定下来了，云终端和虚拟桌面都会去做，具体到用户要看他的需求、条件和实施成本。方向这个东西很重要，因

为一旦定下来就基本没有回头路，比如我们做了7层的访问控制和数据中心，就绝不可能倒退回去。终端虚拟化我们已经着手去做了，三万多个用户分阶段部署，今天一千、明天一千、后天一千地慢慢趋同。

格物资讯：终端虚拟化有拓展到移动设备的计划么？现在技术上好像已经不成问题了。

耿昭：移动端也会做。我们现在部署的深信服的 SSL VPN 有个远程应用发布模块（编者注：即 EasyConnect），它可以把特定应用通过加密隧道推送到移动设备上，并且和终端使用的操作系统类型无关。我们现在只是小规模在用，但它其实可以满足很多业务需求。未来打算往云终端切的时候，我们也可以直接把它当做一个应用做发布，达到和普通电脑类似的效果。

为什么是深信服？

大连电子政务外网中部署了不少深信服的产品，所以在与耿主任的沟通中对该厂商也多有涉及。其实，了解用户对厂商的看法一贯是与用户交流的重要组成部分，是一睹厂商真颜的最佳途径之一。从沟通中可以看出，用户对包括深信服在内的所有厂商是一视同仁的：谁能解决我面临的问题、预见未来将要出现的问题并提供解决方案，自然就能得到我的重视；反之，自然就得不到任何机会。其实与其说是用户给厂商机会，不如说厂商得给自己创造机会。

对于本节内容格物资讯谨保证：1.沟通时未加刻意引导；2.如实记录耿主任的见解。如您仍担心以下内容会令您感到不适，可自行略过。

格物资讯：之前我们了解大连电子政务外网的建设情况时，看到现网运行着很多深信服的设备，您能谈谈选择深信服产品的初衷么？

耿昭：我们 08 年的时候申请了国家信息化专项，要求全系列采用国产自主设备。当时一些国产设备还不成熟，比如负载均衡，到现在一些行业还倾向于用国际品牌。所以在采购前我们先做了个调研，并且希望直接和厂商沟通，很多厂商都是主动打 400 电话过去联系的，其中就包括深信服。后来经过测试，他们产品对需求的满足度还算是比较高的，就放到出口做链路负载均衡，这么多年虽然软硬件都有过升级，但一直算是用住了。

格物资讯：使用中一直没出过什么问题么？

耿昭：一点问题没有也是不可能的，关键是设备没宕过机。如果说上线以后宕掉了，对核心业务造成过影响，那估计后面也就没有任何机会了，我觉得这对任何用户都一样。深信服的设备出过什么问题，比如原来我们做了几千条策略放在里面的时候，发现没有检索功能，真说要找一条策略得一页一页、一条一条的找。我们还没抱怨呢，他们技术人员自己都说这地方得加个检索功能，要不做运维非傻了不可。这个问题其实说明产品功能一定取决于对用户需求的了解，如果是大厂商，他可能有过很多实施经验，就知道这样的需求，于是做到产品里，用户就觉得你很厉害，能想到用户没想过的问题；成长型的厂商可能没有过那么多实施经验，势必要把了解需求、落地到产品里的路走一遍，才能逐渐变成大厂商。所以我和深信服的技术人员开玩笑说，

我们是伴随他一同成长。

格物资讯：您说这个这点我们非常赞同。这几年和一些大型行业用户交流，也听到不少类似的抱怨，比如有用户做数据集中、策略集中以后，发现原有的标称支持六万多条策略的防火墙根本加载不了那么多策略，或者策略超过一定数量以后管理界面总是假死。这应该也说明厂商没有过这种环境下的实施经验，也就发现不了这样的问题。

耿昭：这是一方面，另一方面也是我想说的，有些厂商不太重视用户体验。原来我们也测过一个国内网络安全领头企业的产品，那界面是惨不忍睹，还很不好用。我说你有的页面打开怎么那么慢啊，点一下十几二十秒才能出来，他们配合测试的人就跟我狂解释，这里得统计、得分析才能得到结果。问题是为什么其它产品同样的功能反应就那么快？这有点像手机，苹果的性能不一定比三星、诺基亚好，但它卖的就是用户体验，那是它核心价值很重要的一部分；安全产品里用户体验虽说没有手机那么重要，总也不能太差了，差到让用户用着感觉不方便。

格物资讯：那您感觉深信服产品的用户体验如何？前一阵我们有分析师参加他们的渠道大会，听到有渠道商直接跟他们销售总监抱怨说产品的管理界面“太企业化”，运营商不喜欢。

耿昭：我觉得这恰恰验证了我刚才的说法，运营商认为他产品做得不够，瓶颈不在技术上，是因为他运营商做得少，没有掌握足够多的用户需求。其实很多厂商的产品都一样，核心竞争力往往是都是一堆用户给折腾出来的，功能、性能、易用性都包含在内。深信服产品我的感受是交互做得很好，信息展示比较丰富、管理也很方便，这对我们这样的用户就很重要了。功能、性能肯定不是选型的唯一条件，比如两款产品的应用识别率是 95%和 93%，在用户眼里其实没什么区别。那凭什么选？肯定选易用性好的那个。

格物资讯：关于深信服的产品战略，我们分析师认为他们一直在做一些靠近用户业务的小众产品或跨界产品，绕开了竞争激烈的主战场，曲线做大。不知您怎么看？

耿昭：我觉得这和他们的发展有关，企业规模和市场能力是呈正比的。大企业肯定要做通用的产品，做得越细分越难保证利润；成长型企业你就得去创新，做别人没做过的东西，所以产品不是常态也很正常。但是这种情况不是一成不变的，我之前和深信服老总沟通过，他们现在也开始往大型化去做了，

产品规格在慢慢上移，肯定是被运营商之类的客户催的。不过他们的思路还是比较务实的，可能还是打算在差异化中寻找创新机会。创新是有很大风险，但我觉得不创新也许会让安全厂商消失得更快。有的老牌厂商曾经占据了国内政府行业很大的市场份额，现在几乎看不见了。什么原因？就是因为它总在做老三样，没有什么创新。

格物资讯：您刚才说和深信服的老总进行过交流，能分享一下交流成果吗？

耿昭：我去年 11 月专门到他们公司去了一趟，跟他们老总面谈了一上午。我主要有两个想法，第一是想了解他们企业未来的发展方向，看深信服的产品能不能支撑我们以后的发展，比如他平台的问题，未来能到什么样的处理能力。第二是在了解他们的同时也希望他们能多了解我们，他们对我们需求了解得越多，未来越有可能更好地支持我们。像多设备联动这种想法，就是得不断沟通，才可能产生交集，最终落地到产品。

格物资讯：最后一个问题可能比较尖锐，您觉得深信服产品的优势和不足是什么？

耿昭：优势刚才说了一个用户体验，另一个我觉得可能因为他们是做上网行为管理起家的，对应用的精细化识别做得比较好，有些东西像界面是可以仿制的，但这种还得靠积累。不足的话，第一个刚才其实提过了，他们高端产品规格还得尽快提升。我去深圳的一个重要原因就是要把这块了解清楚，因为选型肯定要考虑未来 3 到 5 年，不能到时候带宽增加了设备却跟不上。其实只要不是出过事故，选型时产品技术路线也应该保证一定的延续性。我们如果把几千条策略从两个不同供应商的产品里倒一遍，技术员得好几天不睡觉来弄，所以说换不起设备。另一个不足不光是深信服的问题，我个人认为国内厂商在产品交互体验、应用管理和 7 层安全方面和国外厂商还有很大差距，还有很长的路要走。这是我实事求是说的话，我跟他们老总也说过这话。

采访后记

之所以选择大连，很大程度上是因为大连电子政务外网建设起步早、进度快、资源整合度高，在业界小有名气。作为示范工程，大连电子政务外网对新理念、新技术、新产品表现出非常开放的态度。经验证后的成功经验，对全国其它地区电子政务外网的建设有着很强的指导意义。

对我们来说，大连之旅是种享受，连番的深入交流让本着学习目的而来的我们感到不虚此行。耿主任身上没有任何官僚气息，他更像一个精通政府行业信息化建设的专家，乐于并善于与人交流分享。由于他超级健谈，且讲出来得皆为干货，给后期整理采访记录造成了很大难度，似乎删掉哪个部分都会影响内容的完整性。鉴于篇幅实在太长，我们最后索性把文章改成对话的形式，尽可能全面、准确地还原每一个细节。

在与耿主任的交流中，有几点令我们印象深刻。首先是业务的崇高地位。大连电子政务外网基础架构建设与运维中的任何决策，都由业务驱动，最终也落地到业务，避免了很多本末倒置情况的出现。业务又从何而来？答案是尽一切手段促进原有独立系统向统一平台迁移，这也是电子政务外网由虚到实的决定因素。而有了丰富的业务，人员角色也要完成从管理者向运营者的转变，才能保证政务与信息化融合的主动性。终极状态下的政务信息化平台，政务和信息化一定是不分家的。

分层、立体化与联动是耿主任谈及大连电子政务外网安全防护工作时出现频率最高的三个词。其实这也不是什么新概念，但罕有用户能将它们捏合成一个强大的防护体系。就像玩植物大战僵尸，玩家会遇到各种各样的敌人，有皮糟肉厚的巨型僵尸（DDoS），有能躲过第一层攻击的梯子僵尸（7 层攻击），还有能穿过防御体系进行反向突破的潜地僵尸（APT）。玩家必须通过手中有限的预算和武器类型，构建出一套合理的防御体系，才能应对千变万化的僵尸组合。大连显然是个有想法的玩家，已经靠自己的理念把游戏打到了难度很高的关卡。不过面对攻击力和种类越来越变态的新型僵尸，其弃终端、保业务的新防护思路还停留在论证试点阶段。希望他们的探索能够成功，将植物大战僵尸的示范工程进行到底。

交流中还有一个印象深刻的地方是用户对产品、技术乃至市场有着深入了解，使其在与厂商关系中的角色发生了改变。大型行业用户与厂商的关系就应该非常紧密，才能把普通的项目变成对双方发展都有益的合作。正如耿主任所讲："厂商对我们需求了解得越多，未来越有可能更好地支持我们。"而对于厂商来说，"产品功能一定取决于对用户需求的了解，如果是大厂商，他可能有过很多实施经验，就知道这样的需求，于是做到产品里，用户就觉得你很厉害，能想到用户没想过的问题；成长型的厂商可能没有过那么多实施经验，势必要把了解需求、落地到产品里的路走一遍，才能逐渐变成大厂商。"

在文章的最后要感谢一下深信服科技，他们为本次采访沟通提供了资源并创造了有利条件。但这并不代表文中涉及深信服的讨论带有软性成分，格物资讯也没有能力去引导、影响或改变采访对象对企业的印象及评价。也欢迎更多的厂商、用户与我们联系，格物资讯会站在用户角度，真实记录并分享更多有价值的用户案例。

版权声明

欲了解更多格物资讯服务事宜，请访问 www.gawainresearch.com，或发邮件至 marketing@gawainresearch.com。