基于终端安全认证和蜜网的跨境企业内网策略浅谈

Discussion on Multinational Enterprise Intranet Strategy Based on Terminal Security Authentication and Honeynet

王　皓（中国农业银行数据中心（北京），北京 100194）
Wang Hao（Agricultural Bank of China Data Center Beijing，Beijing 100194，China）

摘　要：
随着企业的发展，越来越多企业走出国门，设立境外部门，成为跨境企业。而跨境企业建设，不仅面临商业上的困难，同样面对企业网络建设的问题。从跨境企业内网安全角度出发，通过分析普通跨地区企业的网络架构及普通跨地区企业与跨境企业的区别，总结了跨境企业内网建设面临的安全问题，并介绍了一种基于终端安全认证和蜜网技术的接入层控制策略和组网架构，用以提升境外机构内网接入的防护水平。

关键词：
跨境企业；内网安全；终端安全认证；蜜网技术
doi：10.12045/j.issn.1007-3043.2019.04.005
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0021-04

Abstract：
With the development of enterprises，more and more enterprises become multinational enterprises. The development of multinational enterprises not only faces commercial difficulties，but also faces the problem of enterprise network construction. From the perspective of multinational enterprise intranet security，it summarizes the security problems faced by multinational enterprise intranet construction by analyzing the network architecture of common cross-regional enterprises and the differences between common cross-regional enterprises and multinational enterprises. An access layer control strategy and network architecture based on terminal security authentication and honeynet technology is introduced to improve intranet security protection.

Keywords：
Multinational enterprise；Intranet security；Terminal security authentication；Honeynet technology

引用格式：王皓. 基于终端安全认证和蜜网的跨境企业内网策略浅谈[J]. 邮电设计技术，2019(4)：21-24.

0 前言

随着企业市场规模的不断扩大和发展，大量企业开始拓展海外市场，设立境外分公司、加工厂、业务分理处、科研中心等机构。

而现代企业的管理和运营，需要信息系统支持，建立起完善的企业网络，覆盖企业的各个机构。庞大的企业网络需要完备的安全体系进行支撑保障，对企业网络内的信息资源进行防护，保障信息系统的稳定运行。《网络安全法》的颁布加强了对企业网络运维的要求，各企业需遵守网络安全方面的国家标准和行业标准，满足监管机构的各项要求。

跨境企业因其关联方和地理位置的复杂性，面临更复杂的企业网络安全问题。如何防止境外机构遭入侵，如何阻止通过内网连接破坏国内网络系统是跨境企业内网建设必须考虑的内容。

收稿日期：2019-03-01

1 普通跨地区企业网络情况分析

1.1 普通跨地区企业网络结构

大中型企业网络，为保障网络结构的稳定性和可扩展性，便于管理维护，普遍采用层级化网络的模型，由2或3层的结构构成。其中网络的核心层由位于数据中心的核心交换机构成，负责全企业网内部数据的高速交换转发，是全企业网络架构的中心，通常为双机

互为主备互联的冗余设计，对稳定性要求敏感；核心交换机下联各个功能分区的汇聚层交换机，在汇聚层交换机上配置访问控制策略，确保各分区安全，针对重要分区部署防火墙对分区内部资源进行防护；汇聚层交换机下联接入层交换机，与具体用户、服务器等设备相连接，实现用户和服务器的安全接入。

图1为普通跨地区企业（下称普通企业）网络概况。

1.2 数据中心的基本安全措施

数据中心作为企业信息系统资源的核心，汇集了企业最重要的计算机系统、网络设备和配套系统。数据中心内部根据功能划分为多个不同服务器区对企业提供信息系统运维、资料信息存储、业务数据处理、系统应用开发测试、门户网站、邮件系统等服务。企业内网与外网连接的外联区也位于数据中心，通过配置防火墙实现内外网隔离，外网应用由DMZ区提供。外联区采用与互联网连接和与第三方外联等形式。

数据中心内部的网络和服务器设备应严格遵守安全配置规范，严格访问控制，严格账户权限控制，严格执行账号密码管理，配置AAA认证登陆；应部署配置核查和漏洞扫描系统定期对网络设备及服务设备进行安全排查，筛查不合规配置、安全漏洞、弱密码、非必要服务及端口；部署资产清查系统，及时掌握资产增减情况，便于及时定位解决问题；部署服务器、数据库、应用防护系统，防止外部入侵行为破坏篡改；配置审计系统，记录对服务器、数据库、应用系统的配置行为，便于被恶意破坏篡改发生后及时进行回退处理；各分区配置防火墙，对出入分区行为实行访问控制；针对各分区配置IDS系统，分析记录出入分区的疑似攻击行为，及时调整防火墙配置；针对重要系统服务器区配置全流量记录和回溯系统，分析进出分区的流量异常，调整服务器防护策略；定期进行全数据中心的漏洞排查，及时修补漏洞，避免被攻击利用，并定期对全中心进行病毒排查，及时清除病毒、木马等攻击行为。

针对互联网区等外网连接区，面对外部非可信网络，在DMZ区前应配置防火墙、WAF、IDS、IPS，对出入内外网数据深度防护；配置防DDOS攻击系统，防止来自互联网的DDOS攻击造成对外服务瘫痪；配置全流量记录回溯系统，分析来自外部的攻击流量识别已知攻击，并分析未知攻击，及时调整防护策略，阻断攻击行为。

1.3 分支机构的安全措施

图1中分支机构A和分支机构B，与数据中心处于同一国家。分支机构上层的汇聚层交换机，通过专线

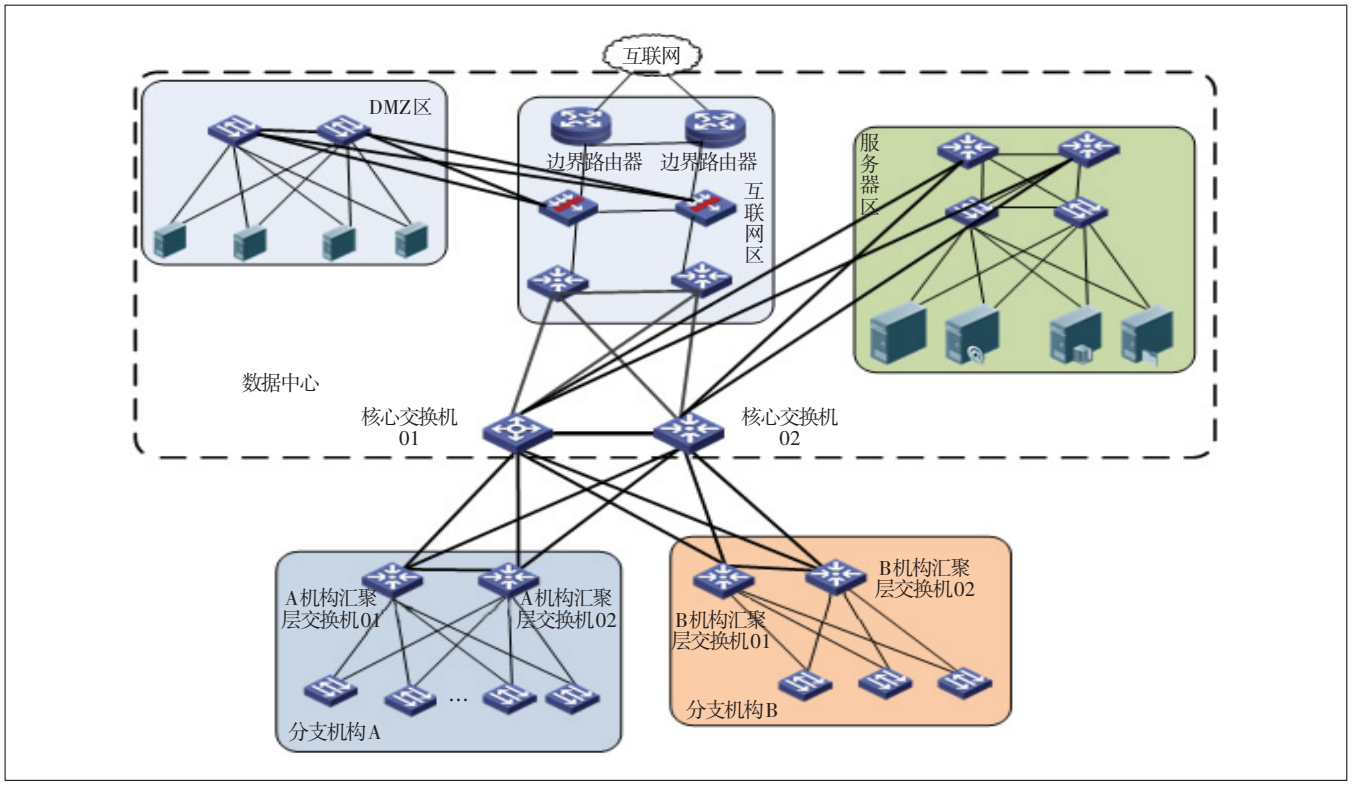

图1 普通企业网络概况

上联数据中心的2台核心交换机；汇聚层交换机下联的本机构内的接入层交换机，分别连接位于机构内不同地点或不同业务需求的本地用户和本地服务器。

分支机构内部网络为汇聚层和接入层，采用以下措施实现对分支机构网络的安全防护：通过在接入交换机上配置端口接入控制，阻断未授权设备接入企业内网；通过对接入交换机下的网段进行访问控制，确保授权用户可访问指定区域；通过对联网设备进行终端安全管理，保证联网设备的主机完整安全和防止信息泄露；通过部署防病毒系统，阻断病毒感染及在网内的传播；通过部署用户行为管理，限制用户进行非法操作，实现对用户行为审计；通过定期安全漏洞检测，及时排查漏洞风险，修复漏洞。

上述措施中的终端安全管理服务器、防病毒系统服务器、用户行为审计系统、安全漏洞检测系统均可部署在数据中心的服务器区，企业内各分支机构通过开通访问权限和所需端口实现功能。

2 跨境企业与普通企业的网络区别

跨境企业与普通企业相比较因机构设置不同，部署形式不同，所面临的监管机构、当地国家或地区法律规定不同，在内网部署方面有较大差异，表1是普通企业与跨境企业内网网络的区别。

表1　普通企业与跨境企业内网网络部分区别

对比项	普通企业	跨境企业
分支机构位置	与总部位于同一国家	分支机构与总部跨国家
监管要求	监管机构要求一致	各地区监管机构要求不一
网络运营商	1~2家	跨多家
分支机构可信度	可信度高	可信度较低
设备供应	相对简单	较为复杂
被监听风险	相对较低	有较高风险

表1中列举了部分跨境企业内网搭建与普通企业的区别，跨境企业搭建内网面临以下困难。

a）地理位置跨度大。与普通企业相比，跨境企业分支机构与总部地理位置跨度较大，甚至跨大洋，给机构间网络部署带来较大困难。

b）监管要求不同。与普通企业相比，跨境企业机构间数据传输将面临所跨越两国的法律约束，如我国《网络安全法》第三十七条、第六十六条都明确规定了关键信息基础设施的运营者在因业务需要提供跨境数据传输所要遵守的相关规定，而其他各国法律也均有对应要求。

c）网络运营商情况不同。普通企业在建设跨地区内网时普遍选择1到2家网络运营商租用专线实现跨地区的数据传输，网络传输质量较稳定。跨境企业机构间建立内网则需在不同国家选择网络运营商，实现跨境数据传输，网络传输质量低于国内专线互联。

d）分支机构可信度不同。与普通企业相比，跨境企业因环境背景复杂，其网络被渗透被攻击可能性加大，因此需对境外机构连接企业内网设置专用的DMZ区进行隔离。

e）设备供应情况不同。普通企业设备资产和服务采购，同类别产品可采购统一供应商，全部分支机构设备统一配备，减轻后期运维压力。且根据监管规定，出于安全需要，可全部选择或重要敏感部分选择自主可控品牌搭建企业网络。跨境企业因供应商服务能力和经营国家地区范围，在境外可能无法选择与国内相同的品牌，且部分国家也要求信息系统需选择当地供应商或监管机构批准使用品牌，给组网带来一定的不便。

f）被监听风险不同。与普通企业相比较，跨境企业因其商业价值受到境外国家政府、监管、企业的层层关注，传输线路数据存在被监听风险，且因设备资产采购于境外供应商，存在被后门监听的可能。

g）时差、文化等其他差别。跨境企业国内总部与境外分支机构普遍存在时差，对网络联合调配造成不便；境外所在国家与国内存在文化差异，且因人员配备需要有部分外籍雇员，外籍雇员与国内技术人员的沟通理解有一定不便。

3 终端安全认证和蜜网的境外机构内网防护

分析境外分支机构面临的安全问题，部署终端安全防护系统和蜜网服务器在终端接入层设置防护，保护内网真实环境。

3.1 系统架构

本系统在境外分支机构接入层交换机部署终端安全服务器、radius认证服务器以及入侵检测系统IDS，在接入层交换机与汇聚层交换机间部署深度检测防火墙，并部署honeynet蜜网服务器群。

图2为基于终端安全与蜜网的境外机构内网架构。

数据中心部分单独设立境外连接区，通过境外DMZ区隔离境外与内网的连接，在边界路由器通过境内境外专线连接至境外分支机构边界路由器。

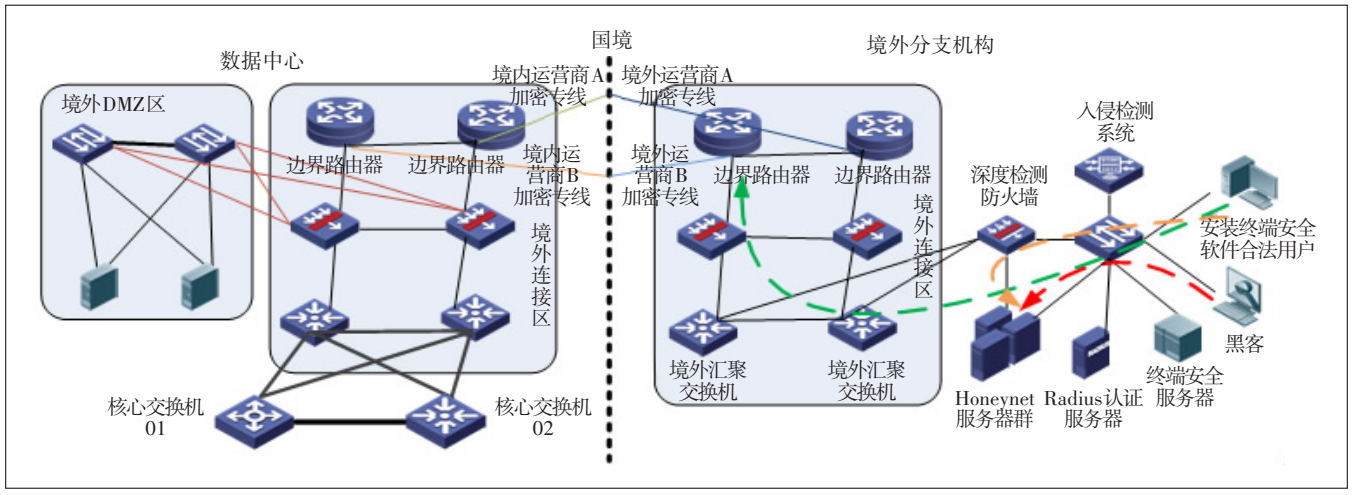

图2 基于终端安全与蜜网的境外机构内网架构

境外分支机构设置与数据中心境外连接区对称的汇聚层结构，边界路由器下联防火墙，防火墙向下连接汇聚层交换机。

汇聚层交换机与接入层交换机间设置防火墙，并配置honeynet服务器区。honeynet服务器区内部配置多层虚拟网络结构和多分区，设置honeypot迷惑攻击者，分支机构接入层交换机连接终端安全服务器、radius认证服务器和IDS，保障接入层可控。

3.2 接入层控制策略

所有内网合规用户均须在终端上安装终端安全系统，配置强制合规策略，检查被管理终端是否存在漏洞，是否安装防病毒系统，是否安装黑名单软件。

a）当有终端连接至接入层交换机其上联端口并不允许传输数据，终端需将终端安全系统检测的强制合规信息上传至终端安全服务器，并将其认证信息发送至radius服务器，在通过终端安全强制合规检测和认证通过后，放行向内网传输数据，在传输过程中，如无异常行为，则保持与内网连接。

b）当可疑终端连接至接入层交换机，未能满足强制合规或radius认证时，接入层交换机将不允许终端接入内网，而将可疑终端连接至honeynet服务器群的“仿真”内网环境，并监测可疑终端是否在honeynet开展攻击行为，如检测到攻击行为则中断连接。

c）当设备通过强制合规监测和radius认证，而在连接过程中经IDS或深度检测防火墙发现可疑行为时中断其访问内网，并将其引入honeynet服务器群，当可疑行为继续进行时，将标记该设备为疑似受控设备，并与终端安全服务器联动否定其强制合规监测，下次连接将不再让其连接内网。

通过引入接入层控制策略，将防止黑客直接接入境外内网或控制合规终端进入内网，对内网资源进行破坏。

4 结束语

综上所述，在境外机构内网接入层进行终端安全认证和蜜网策略部署可有效防护黑客直接接入境外内网或控制内网合规终端，对内网资源安全防护有重要意义。在网络系统建设中面临的诸如传输过程中网络监听、人为物理破坏等攻击行为仍需要通过技术和管理体制的完善去不断克服解决。

参考文献：

[1] 周文. 浅谈企业内部信息网络安全防护体系建设[J]. 网络安全技术与应用，2014(5)：166-167，169.
[2] 胡文华. 冲击与应对：GDPR与《网络安全法》比较视野下的企业合规[J]. 中国信息安全，2018(7)：77-81.
[3] 张瑞睿. 关于计算机网络安全防范技术的研究与应用[J]. 科技创新与应用，2018(35)：173-174.
[4] 王少强. 城市商业银行数据中心建设与管理分析[J]. 管理观察，2019(1)：158-159.
[5] 宣增. 紫金数据中心互联网安全接入解决方案[J]. 中国金融电脑，2019(1)：87.

作者简介：
王皓，毕业于华北电力大学，助理工程师，硕士，主要研究方向为信息安全漏洞排查相关领域。