文章编号：2096-1472(2021)-01-32-03
DOI:10.19644/j.cnki.issn2096-1472.2021.01.009

运用虚拟桌面技术实现跨网络边界的安全访问

龚 伟

(中车株洲电力机车有限公司运营与信息管理中心，湖南 株洲 412000)
✉gongwei.zz@crrcgc.cc

摘 要：随着网络安全被提升到国家战略，企业逐步开始对信息网络进行边界隔离改造，划分不同网络区域，因此带来了隔离网络间系统访问、用户管理的挑战。本文采用虚拟桌面技术，研究规划在多个隔离网络边界环境下，实现跨网络边界安全访问的可行性。经企业环境推广验证，本文所研究的方法能够使企业实现统一管理、按需交付的跨网络边界安全访问平台。文中所涉及的方法和技术，可以为企业在网络安全加固保护、信息安全和用户管理层面提供全新的思路，提升企业信息安全水平。

关键词：虚拟桌面；网络边界；安全访问；身份鉴别
中图分类号：TP309.1 **文献标识码**：A

Secure Access Across Network Boundaries with Virtual Desktop Technology

GONG Wei

(*Operations and Information Management*, *CRRC Zhuzhou Locomotive Co.,Ltd.*, *Zhuzhou* 412000, *China*)
✉gongwei.zz@crrcgc.cc

Abstract: As network security has been promoted as a national strategy, enterprises gradually begin to transform information network boundary isolation and divide different network areas. This brings challenges to isolating system access between networks and user management. This paper uses virtual desktop technology to study feasibility of achieving secure access across network boundaries in multiple isolated network boundary environment. Proved by enterprise environment promotion, the proposed method can realize unified management for enterprises and a secure access platform across network boundaries, that is delivered on demand. Methods and technologies involved in this article can provide enterprises with new ideas in network security reinforcement protection, information security and user management levels, and improve the level of enterprise information security.

Keywords: virtual desktop; network boundary; secure access; identity authentication

1 引言(Introduction)

大型企业信息化建设中，为了确保信息系统安全性，通常会将信息化网络拆分为多个专用网络，从而形成边界隔离的网络环境，不同边界间使用防火墙、网闸或者物理隔离的方式，实现访问控制和安全策略管理[1,2]。但企业计算机设备、应用系统一般仅允许连接到一个网络区域中，员工无法使用单一终端接入多个网络，使用不同网络中的应用系统[3]。传统情况下企业会为用户配置多个终端，然后使用键盘显示器鼠标(Keyboard Video Mouse，KVM)切换器进行多计算机统一控制[4]，但此种方式存在成本高昂、难以管理、易形成安全风险的问题。随着虚拟桌面技术不断成熟，终端、用户、桌面分离管理，后台统一配置交付的技术方案，为企业实现跨网络边界安全访问提供了富有价值的解决方案。本文运用虚拟桌面技术，设计并实现了一套跨网络边界安全业务访问系统平台，经企业实际场景推广运行，为企业员工访问不同网络区域中的信息系统，提供了安全可行的解决方案。

2 多网络边界虚拟桌面架构(Multi-network boundary virtual desktops architecture)

虚拟桌面技术已在信息技术领域中推广应用多年，企业为确保解决方案的稳定性，以及产品的支持服务，通常会选择使用较为成熟稳定的虚拟桌面解决方案产品，如思杰XenDesktop、威睿Horizon View及微软RDS等产品[5]。本文

采用思杰XenDesktop产品作为技术支撑，按照跨网络边界安全访问的需求，进行架构设计、服务配置和用户虚拟桌面交付[6]。企业按照信息化规划，将不同业务领域的信息网络，根据业务数据流转规则[7]以及云计算环境下的实际环境，规划包含生产专用网、研发涉密网、普通办公网以及公共互联网在内的四个网络边界区域，每个网络均采用信息网络技术加以隔离保护，每个网络边界区域功能定义如表1所示。

表1 网络边界区域功能定义

Tab.1 Network boundary area functional definition

网络区域	区域功能	边界隔离方式
生产专用网	生产制造业务运行网络	网闸，物理隔离
研发涉密网	研发设计人员设备专用网络	网闸，物理隔离
普通办公网	职能办公网络	防火墙，逻辑隔离
公共互联网	互联网区域网络	防火墙，逻辑隔离

根据企业的网络边界区域划分，基于虚拟桌面技术采用集中式管理、统一虚拟桌面交付的特点，本文所设计的跨边界网络安全访问虚拟桌面架构如图1所示。图1中，虚拟桌面服务资源按照就近原则放置在各网络区域中，并且不改变企业现有网络边界区域划分，在特殊隔离区域之间，配置虚拟桌面网关设备(实现虚拟桌面访问会话加密代理服务)。并在虚拟桌面接入终端设备上部署定制化身份鉴别接入程序，访问企业统一虚拟桌面门户，由虚拟桌面后台服务判断终端的源和目的网络边界区域，分配授权可访问的虚拟桌面，以及应用虚拟桌面安全策略实现用户终端跨边界网络安全访问需求[8]。

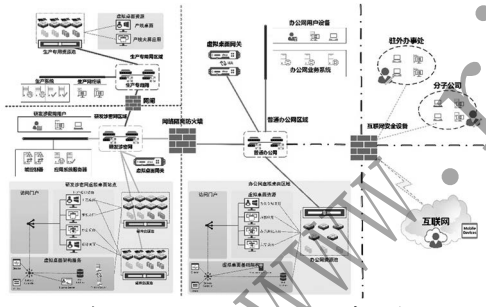

图1 跨边界网络安全访问虚拟桌面架构图

Fig.1 Cross-border network security access to virtual desktop architecture diagrams

3 跨网络边界安全访问模型(Secure access model across network boundaries)

通过虚拟桌面技术实现的跨网络边界安全访问功能，首先可以保障用户通过统一的门户进行多个网络区域内资源的访问、切换；其次，用户终端可采用定制化终端接入程序，将客户端设备均默认配置为零信任(Zero-Trust)状态，再由后台身份鉴别服务进行鉴别后提供服务。最终实现零信任统一安全访问模型，所有终端用户均访问统一的虚拟桌面平台门户，门户与终端之间采用HTTPS加密传输，用户虚拟桌面会话采用安全数字证书加密的虚拟桌面会话交付。在高安全性要求的两张网络之间，采用加入双因素(Two-Factors)身份认证，并判断客户端健康状态方式，确保终端、用户均可以受控，安全可靠。图2中所展现的终端与虚拟桌面的安全访问模型，为本文所规划配置的目标状态。

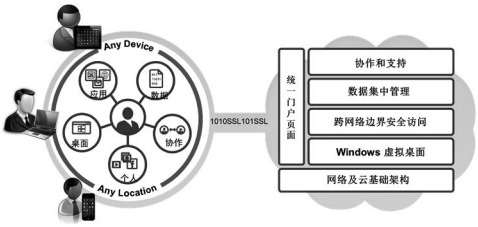

图2 跨网络边界安全访问模型

Fig.2 Secure access model across network boundaries

当用户访问不同边界网络区域时，所需采取的身份鉴别认证方式也不同，该边界网络区域内所提供的虚拟桌面服务类型也需根据实际情况进行区分，表2描述了访问模型中的区域安全访问列表配置。

表2 区域安全访问列表

Tab.2 Area security access lists

网络区域	区域认证方式	提供服务
生产专用网	终端认证、用户认证	池化桌面
研发涉密网	终端认证、用户认证、双因素认证	专属桌面
普通办公网	用户认证、双因素认证	池化桌面
公共互联网	用户认证	池化桌面

4 虚拟桌面安全策略设计(Virtual desktops security policy design)

思杰XenDesktop平台中，针对虚拟桌面安全策略，可以根据用户不同的接入设备、接入方式，以及所访问的不同虚拟桌面类型进行控制和调整[9]。通过安全策略配置可以实现以下各项安全功能：

(1)剪贴板数据传递限制。

(2)终端设备磁盘映射，访问权限控制。

(3)虚拟桌面显示/隐藏安全控制。

(4)本地打印机调用安全控制。

(5)显示虚拟桌面水印，动态防截屏控制。

(6)USB、COM、串口等外接设备安全控制。

如表3所示的策略配置表描述了配置选项：启用、禁用、允许、禁止和未配置。

表3 策略配置表

Tab.3 Policy settings table

终端网络	目标网络	安全策略
公共互联网	普通办公网	允许访问
	研发涉密网	允许双因素认证后访问，并启用安全控制功能
	生产专用网	禁止访问
普通办公网	公共互联网	开放访问
	研发涉密网	双因素认证，并启用安全控制功能
	生产专用网	双因素认证，并启用安全控制功能
研发涉密网	公共互联网	禁止访问
	普通办公网	允许访问，并启用安全控制功能
	生产专用网	允许双因素认证后访问，并启用安全控制功能
生产专用网	公共互联网	禁止访问
	普通办公网	禁止访问
	生产专用网	允许访问，并启用安全控制功能

5 终端用户身份鉴别设计(End-user identity authentication design)

虚拟桌面的接入使用，需要利用各类型的用户终端设备，如瘦客户机、台式计算机、笔记本电脑、移动平板等。由于本方案中存在多个网络边界区域，需要针对不同区域接入虚拟桌面的终端，执行不同的安全策略，分配不同的虚拟桌面资源，因此需要进行终端用户身份鉴别处理。本文采用定制化终端接入程序[10]，实现对终端设备所处网络边界、用户身份及终端设备安全性的检测。整个终端用户身份鉴别业务流程示意图如图3所示。

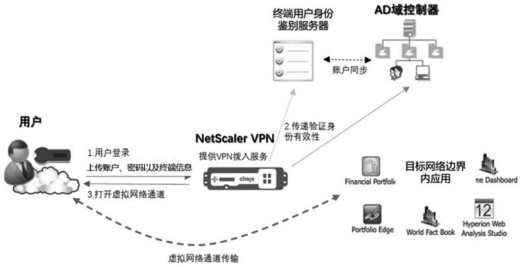

图3 终端用户身份鉴别流程示意图

Fig.3 A diagram of the end-user identification process

身份鉴别服务端部分伪代码：

(1)创建终端用户身份账户数据库。

(2)创建终端设备计算机名、IP地址匹配规则。

(3)接收定制化终端接入程序提交的终端计算机名、IP地址、账户和密码。

(4)比对终端用户身份、计算机名和IP地址，匹配对应的访问页面。

(5)使用思杰标准API接口，向StoreFront服务器传递用户账户、密码，获取用户虚拟桌面资源列表。

(6)将虚拟桌面资源列表发送到定制化终端接入程序。

(7)结束与终端程序服务连接。

定制化终端接入程序部分伪代码：

(1)启动程序，获取终端设备计算机名、IP地址，判断是否安装安全软件，若安装则继续，否则提示并退出。

(2)返回登录界面窗口，由用户输入账户、密码，将用户名、密码提交到后台服务器。

(3)获取虚拟桌面后台服务器返回的虚拟桌面资源列表。

(4)用户选择需要访问的虚拟桌面资源，程序调用虚拟桌面客户端思杰Receiver插件。

(5)Receiver插件连接虚拟桌面，并应用虚拟桌面安全策略。

(6)定制化终端接入程序退出。

根据上述代码逻辑，定制化终端接入程序效果如图4和图5所示。

图4 定制化终端接入程序效果图

Fig.4 Effect map for customized terminal access program

图5 虚拟桌面资源展示效果图

Fig.5 Presentation map of virtual desktops resource

6 结论(Conclusion)

本文提出了企业在信息安全要求日益严峻的情况下，部署多网络边界区域环境，为实现用户终端跨网络边界安全访问的需求，运用虚拟桌面技术和终端身份鉴别技术，设计的一套单一设备、多网使用、安全控制、统一交付的解决方案。通过在企业生产环境中的应用部署，对本文所述方案进行了效果验证，相较于传统计算机终端，采用虚拟桌面技术后，员工工作便捷性和终端桌面维护工作效率均得到大幅度提升。由此说明，虚拟桌面技术在实现跨网络边界安全互访的需求中，具有充分的可用性、易用性，满足用户可以扩展到其他具有相同需求的企业场景中进行推广的需求。

参考文献(References)

[1] 马骁.基于信息安全的网络隔离技术研究与应用[J].电子元器件与信息技术,2020(05):26-27.

[2] 刘赫.基于网络安全等级保护2.0的安全区域边界[J].电子技术与软件工程,2020(01):236-238.

[3] 张克贤,钟掖,张光益.计算机网络边界安全防护管理方法研究[J].通讯世界,2019(12):80-81.

[4] 白宁.让复杂变简单:体验KVM多电脑切换器[J].网络与信息,2012(01):52-53.

[5] 马博峰.VMware、Citrix和Microsoft虚拟化技术详解与应用实践[M].北京:机械工业出版社,2013.

[6] 刘宸,王强.基于Citrix虚拟化的桌面云平台构建与应用研究[J].智能计算机与应用,2017(10):98-99;103.

[7] Laisen Nie, Dingde Jiang, Zhihan Lv. Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks[J]. Annals of Telecommunications, 2017(72):5-6.

[8] 武越,刘向东,段翼真.桌面虚拟化安全访问控制架构的设计与实现[J].计算机工程与设计,2014(05):1572-1577.

[9] 骆慧勇.基于云桌面实现网络安全隔离的应用[J].计算机应用与软件,2020(2):16-17.

[10] 傅鹂,郑宇,黄小明.综合身份鉴别系统的研究与开发[J].软件导刊,2006(19):59-61.

作者简介：

龚 伟(1979-)，男，硕士，高级工程师.研究领域：制造业信息化，企业信息化管理.