# 钢铁企业基于零信任网络安全体系的搭建与应用

文◆唐山钢铁集团有限公司　张宝玉　孙　博

## 引言

随着钢铁企业智能制造建设的不断深入，企业园区网络的规模和覆盖范围不断扩大，给企业发展带来新机遇的同时，也为企业的网络安全工作带来了巨大的挑战。移动互联网、工业互联网、云技术、大数据等信息技术的广泛应用，使网络安全边界变得更加模糊，网络安全形势日益严峻。新型病毒、木马和网络攻击方式层出不穷，传统网络安全防御方式失效，无法保障企业IT资源的安全。移动办公的普遍应用是因为传统的网络访问控制策略难以执行。移动互联网的普遍使用，使企业面临的内部和外部网络安全威胁同样严峻，由于内部网络限制较少，网络威胁更容易横向扩散。因此，传统的基于边界防御的网络安全架构已经不能满足网络安全管理的需要，基于零信任的架构成为解决传统网络安全架构问题的有效方法。本文结合实践，介绍了一种在不同网络区域采取适用网络安全技术搭建基于零信任网络安全系统的方法。

## 1 零信任的概述

2010年，著名研究机构Forrester首席分析师约翰·金德瓦格（John Kindervag）首次提出了零信任安全的概念[1]，即所有的网络流量和网络访问都是不可信的，任何的访问请求都需要进行安全验证和授权。零信任概念的提出是对传统的基于安全域划分、安全域隔离为基础的网络安全防御理念的颠覆[2]。

在传统的网络安全体系中，防御的重点在于网络边界和来自外部的网络威胁，而对园区内部网络的用户和访问则认为是安全的，限制较少，这已经不再适合现有日益复杂的网络安全形式。基于零信任的安全概念认为对网络资源的访问始终是“不可信的”，不默认任何访问安全，不对任何访问进行默认授权，需要持续验证网络访问的安全性。

零信任架构的目标是保护企业的每一个资源，而不是保护内部网络的安全边界[3]。零信任的网络安全体系遵循零信任的理念进行设计，具有全面用户安全认证、最小化访问授权以及动态网络威胁监测和反馈等特点。零信任的网络安全体系可以对访问主体实现未授权资源的隐身，缓解或解决网络安全威胁、风险和漏洞等问题。因此，零信任的网络安全体系能缓解或解决传统网络安全架构所面临的问题，进而保护企业IT资源的安全。

## 2 零信任安全体系的组成和应用

根据企业网络数据通讯需求，搭建基于零信任的网络安全体系，不能仅依靠单一的设备或系统实现，需要根据不同应用场景的特点，采取

【作者简介】张宝玉（1975—），男，河北唐山人，硕士研究生，正高级工程师，研究方向：信息系统集成、网络安全。
【通讯作者】孙博（1985—），男，河北唐山人，本科，高级工程师，研究方向：冶金自动化。

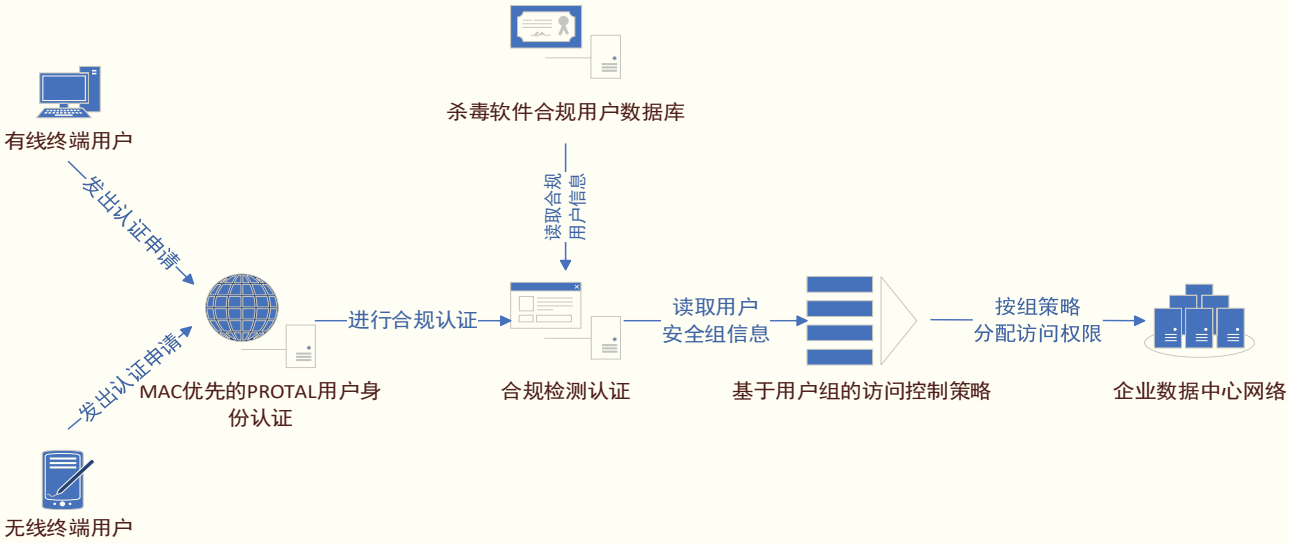


图 1 基于零信任的园区网络用户准入控制逻辑图

适用的网络安全技术才能实现。

**2.1 园区网用户零信任安全管理系统**

企业园区网用户无疑是企业最庞大和复杂的网络用户团体，需要采用既全面又高效的零信任管理模式。通过实践验证，应用了包含身份认证、合规监测和访问授权三合一的验证模式。

基于零信任的园区网络用户准入控制逻辑图如图 1 所示。

需要特别说明，在用户访问控制授权环节应采用基于组策略的访问控制方式，以满足移动办公和动态授权控制的需要。同时，访问授权的方式基于白名单，即没有明确的访问需要默认为不予授权访问。

**2.2 外部接入用户零信任安全管理子系统**

随着互联网的发展，企业外部职工、客户和合作伙伴等通过互联网访问内网的需要在不断增加。保障外部用户安全接入内部网络工作是企业网络安全管理中的重要一环，推荐使用“VPN+ 堡垒主机”的安全管理模式。VPN 实现身份认证、加密通讯、内网资源定义和授权访问等功能。堡垒主机实现代理登录、资源授权、行为记录和审计，避免外部终端与内部资源之间数据交换，避免包含内部资源的账号和密码泄漏，同时对外部用户的访问行为进行记录、保存，保持可追溯性。

**2.3 子分公司及互联网接入零信任安全管理子系统**

大型钢铁企业中，“一业多地”的生产模式已经成为常态，子分公司之间以及与总部之间的数据通讯需要在所难免，采用基于白名单的七层防火墙管控模式，按照需要在防火墙上建立基于应用的访问白名单。开启网络威胁监测和漏洞防护功能，阻断一切非必要的网络通讯，形成零信任的子分公司网络安全管理子系统。

互联网接入历来是安全防护的重点，除了外网防火墙外，对外发布的应用系统因部署 Web 应用防火墙，形成安全访问基线，拒绝一切非基线访问行为。同时，在互联网出口部署安全沙箱系统，用于迷惑黑客和捕获网络攻击行为。

**2.4 工业控制网络零信任管理子系统**

随着智能制造的不断深入，钢铁企业产线自动化、网络化和智能化水平不断提高。同时，各产线工业控制网络横向通讯需求和管理网络的纵向通讯需求日益增加。基于零信任网络安全理念，需要在各产线工业控制网络之间和工业控制网络与管理网络之间增加基于白名单的防火墙，采用能够识别和支持工业网络通讯协议的工业防火墙，根据需要开通指定应用的网络访问白名单，禁止一切非必要网络通讯，保护工业控制网络的安全性。

**2.5 数据中心主机及应用软件零信任管理子系统**

数据中心主机及应用软件系统是安全防护的重点部位。基于零信任的网络安全理念，需要结合应用系统的特点制定相应的安全机制，主要安全措施包括系统的高可用措施（双机热备，负载均衡等）、系统和数据的备份恢复机制、系统的代码审计、漏洞扫描、渗透测试、邮件审计机制

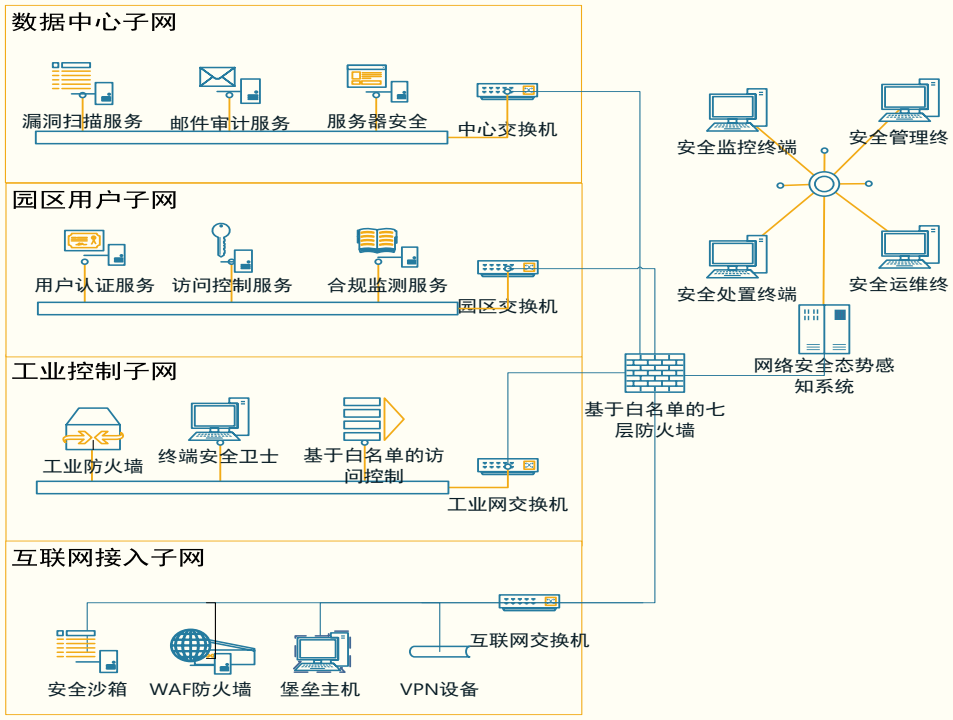


图 2 各区域基于零信任的安全技术应用示意图

等，保证业务的连续性和系统、数据的安全性，采取主动的安全措施保护系统安全。

**2.6 态势感知、流量分析主动检验修正安全策略**

基于零信任的安全控制策略的有效性和合理性需要通过实践进行检验。在外网出口、网络核心、数据中心、工业网核心、子分公司专线等关键部位部署网络安全态势感知系统和网络全流量分析系统。态势感知系统可用于存在威胁的外部网络攻击和内部网络威胁行为的分析和判断，修正现行的网络安全策略，关闭或修正存在威胁的网络访问。网络全流量分析系统可对网络带宽占用情况和网络通讯质量进行分析，发现网络通讯中的瓶颈和不合理的通讯带宽占用，保障高质量的网络通讯。

## 结语

针对不同的网络区域，基于零信任安全理念应采取不同的安全技术，各区域基于零信任的安全技术应用示意图如图 2 所示。各种技术的综合应用，旨在不同网络区域形成零信任的安全网络体系，全面识别和保护网络应用和用户，限制非法访问和应用，防范已知和未知的网络威胁，保护网络资源。

传统网络安全架构假设企业内部网络可信，注重在网络安全边界进行防御。这种信任增加了安全风险，使得传统网络安全架构难以有效防御新型网络攻击。基于零信任的网络安全的理念，有效缓解或解决了传统网络安全架构存在的问题，已经成为网络安全领域的重要发展趋势。

## 引用

[1] 算网融合产业及标准推进委员会.零信任技术和产业发展(2022年)[R/OL].(2022-12-15)[2023-1-15]:http://www.ccnis.org.cn/Assets/file/whtiepaper/lingxinrjscyfz.pdf.

[2] 余海,郭庆,房利国.零信任体系技术研究[J].通信技术,2020,20(8):2027-2028.

[3] SIMPSON W R,FOLTZ K E.Maintaining Zero Trust with Federation[J].International Journal of Emerging Technology and Advanced Engineering,2021,11(5):17-32.