学号 12202400203

湖南理工学院

毕业综合训练(论文）

题目: 企业园区网安全技术及应用研究

作　　者	袁博	届　　别	2024 届
院　　别	信息科学与工程学院	专　　业	计算机科学与技术
指导教师	周细义	职　　称	副教授
完成时间	2024 年 4 月 24 日		

摘　要

企业园区网络已成为企业日常运营、管理的重要基础设施，也是国家安全中网络安全的重要组成部分。数据泄露、恶意攻击、服务中断等，这些安全问题不仅威胁到企业的信息安全，甚至对于基于企业服务的群众生活支付、服务等造成影响。本文首先进行企业园区典型网络搭建，包括网络需求分析、设计思路阐述和网络安全方案初步设计，并完成企业园区网络模拟。其次，通过部署 WAF、蜜罐、堡垒机等安全设备来提升网络的安全防护能力。最后，从接入安全、传输安全、数据安全三个方面，进行网络安全协议层面的基本测试以及蜜罐等安全技术的基本功能测试。总结了企业园区网安全技术及应用研究的成果和不足，并对未来先进网络安全技术进行展望。

关键词：网络安全、访问控制、蜜罐、安全设计、堡垒机

Abstract

The enterprise park network has become an important infrastructure for daily operation and management of enterprises, and is also an important component of network security in national security. Data leakage, malicious attacks, service interruptions, and other security issues not only threaten the information security of enterprises, but also have an impact on the payment and service of people's lives based on enterprise services. This article first conducts a typical network construction for enterprise parks, including network demand analysis, design ideas, and preliminary design of network security solutions, and completes network simulation for enterprise parks. Secondly, by deploying security devices such as WAFs, honeypots, and bastion machines, the network's security protection capabilities can be enhanced. Finally, basic testing of network security protocols and basic functional testing of security technologies such as honeypots will be conducted from three aspects: access security, transmission security, and data security. Summarize the achievements and shortcomings of enterprise park network security technology and application research, and provide prospects for future advanced network security technologies.

Key words: Network security, access control, honeypot, security design, bastion machine

目　录

第 1 章 绪论

1.1 研究背景和意义

（1）研究背景

随着自动化程度越来越高，网络的基建属性越来越强，人们吃、穿、住、用、行都离不开各类企业基于网络进行的相关服务，企业园区的内外的网络安全便显现的愈加重要。

随着信息技术的迅猛发展和网络应用的广泛普及，企业园区网的安全问题日益突出。网络攻击、数据泄露等安全事件频发，对企业信息安全和业务发展构成严重威胁。因此，加强企业园区网安全技术及应用研究具有重要的现实意义。从 21 世纪以来，国外 Slammer 蠕虫病毒导致数百万 SQLserver 的数据库感染、“震网”病毒导致伊朗离心机工控系统故障、勒索软件“WannaCry”爆发利用 NSA 的后门漏洞传播造成重大社会影响；国内新网域名解析服务器攻击、大型门户服务器被侵入、中国人寿保单信息泄露等等信息泄露、基础设施服务中断现象层出不穷。

在国家安全角度上，近 3 年以来的网络安全事件也不少。军事中 2022 年 6 月西工大遭受疑似 NSA 的网络攻击，利用“二次约会”间谍软件及其衍生版本进行攻击造成数据泄露；民生中，拼多多、淘宝等购物、团购服务平台经常遭受拖库攻击造成用户数据泄露；社会中，武汉地震局地震采集台站网络设备被入侵在特殊时期的误报或漏报会造成难以想象的影响。

虚拟化云服务、Lot 物联网、大数据分析等各类新技术在企业园区网中的广泛应用，为企业带来了更高效、便捷的服务，但同时也带来了新的安全挑战。因此，研究新技术背景下的企业园区网安全技术及应用，对于保障企业信息安全、推动新技术应用具有重要意义。企业园区网络，他的特点便是带宽规模较大、资源共享度高、终端设备多且聚集，一但发生网络安全事故极有可能造成企业整体业务中断、大量客户个人信息、员工个人信息以及科研方向的敏感数据造成泄露。因此，企业园区网安全技术的研究以及与时俱进显得极为重要。

（2）研究意义

对于企业园区网安全技术及应用研究的研究意义主要有以下四个方面：

1.解决当代企业园区网的基本搭建问题。

当代企业园区网搭建过程中将面临不同对象、不同平台、不同基础设施、不同系统等搭建难题，各种不同需求相互交织。本文将根据典型企业园区网进行部署，满足生产网、研发网、办公网、监控网等各类不同 IT 网络平台环境需求的主干搭建问题。同时，引入服务器群、虚拟化平台、云平台、中间件群（Rancker

搭建的 Docker 群）等新兴技术，并针对性对新兴技术带来的安全隐患进行剖析并提供相应解决方案。

2.防范企业园区网络可能存在的网络安全隐患。

通过调研，当前的企业网络可能存在的网络安全隐患，主要分为七个板块：信息泄露（数据泄露）、未经授权的访问、破坏信息完整性（WEB 服务器配置等）、钓鱼网站、病毒威胁、特洛伊木马和社会工程攻击，总体来讲“三分防、七分管”，本文将在“三分防”的部分重点研究，同时根据网络协议进行安全测试。

在后文中将根据信息泄露、未经授权的访问、破坏信息完整性（WEB 服务器配置等）、钓鱼网站、病毒威胁、特洛伊木马和社会工程攻击的相应七个板块，信息加密技术防止数据泄露、数字签名和身份认证技术验证授权访问、访问控制技术防止越权操作、反病毒技术进行扫描和路由数据、数据库数据进行备份与恢复等主要安全技术进行初步探究。

3.研究应用到企业园区网的具体安全技术。

企业园区网应用的具体安全技术一般有：WAF 技术、IPS 技术、VPN 技术、蜜罐技术等，主要解决数据安全、网络流量安全、访问安全等三个方向问题，本文也将在这三个方向问题中进行重点研究，同时根据“零信任”的理念及内部网络脆弱的大环境，引入“零信任”理念及接入方案，尝试“零信任”SDP 接入方案取代正反向代理的可行性，解决 VPN 来自公网攻击的风险。

4.深化企业园区网安全管理方法及对未来新兴技术展望。

企业园区网安全管理的重要举措对于当代网络安全“三分防、七分管”的基本理念非常重要，在人员安全教育及风险操作提醒中下足文章。同时根据业务服务中的与外网有关的（FTP、邮件、WEB 等）进行重点管理管控。在新兴技术方面，针对云技术：中间件群、虚拟化平台等相关的网络安全技术及人工智能检测恶意邮件、文件、代码及流量等方面进行针对性展望及初步探究。

1.2 国内外研究现状

（1）国内研究动态

在国内，企业园区网安全技术及应用研究得到了广泛的关注，关于网络安全方向主要分为网络安全防护体系研究、云计算安全技术研究、工业控制系统安全研究和人工智能在网络安全方向的应用研究四个方面：

在网络安全防护体系研究方面，奇安信学者张泽州、王鹏在谷歌的 Beyond Corp 项目的基础上根据国内企业数字化转型深入、各企业网络结构日趋复杂的现状下提出了零信任理念[1]的安全思路，通过持续认证的基本思路为网络安全打开新局面；不同于安全事件生命周期管理的 PDR2A 的网络安全防护体系思路，

蒋宁等五名研究人员[9]在物联网、工控网等内部局域网基础上提出基于 IPDRR 网络安全管理模型的安全可视化运维思路，同时在防火墙、入侵检测、数据加密等方向进行了规范，针对技术和管理两个方面进行了长足研究，对国内保密局域网网络安全防护体系研究方向有进一步推动。

在云计算安全技术研究方面，童威,黄启萍两位学者[2]针对云储存的传输、访问、隔离、销毁、储存进行概况同时对于安全方面的 VPN 等传输技术加解密方式及达梦等数据库国产化和多点备份技术进行了多方位阐述；从 2021 年以来 Kvm、Xen 到 Docker 及 K8s 等虚拟化软件带来的模糊开发和运维的服务被广泛应用于国内，同时也带来了安全问题，金华松[3]在虚拟机逃逸攻击、虚拟机间攻击和资源竞争 DDOS 攻击方面做出的详细问题剖析，并针对性提出虚拟机隔离加密加固、网络安全监控等方式进行虚拟化安全管控；同时云访问安全也是重点研究方向，刘奇旭,靳泽,陈灿华等多名学者[4]详细阐述了工控、智慧家居等物联网安全方向上的访问控制风险点，并提出了引入“零信任”持续认证概念的访问控制理念。

在工业控制系统安全研究方面：随着工业 4.0 的推进，工业控制系统安全成为企业园区网安全的重要组成部分。孙彦斌,汪弘毅,田志宏等多名学者[5]针对工业控制系统的漏洞挖掘、安全防护和入侵检测等方面，进行了详细阐述，包括工业信息系统因采用“万国造”导致如 RS-232、RS-485、CAN、Modbus、PROFINET、Modbus TCP、UMAS、S7comm、S7comm-Plus、PPI、DNP3、Omron FINS、Melsec 等多类别的网络通信协议引发的工业控制协议攻击和隐蔽的上位机攻击，并提出了工业控制系统网络方向的安全防护任务和关键技术攻关路径。

人工智能技术在网络安全中的应用研究中，李向东学者[6]利用人工智能技术检测恶意代码为 Web 安全及恶意软件识别提供了相关路径；任华学者[7]基于网络安全事件提出了网络安全威胁识别，为快速预警、处置高危事件提供了相关预测路径；同时陈明,汤文峤学者[8]提供了网络威胁情报分析的相关路径。

（2）国外研究动态

在国外，企业园区网安全技术及应用研究同样受到广泛关注。近年来，国外的研究主要集中零信任网络安全模型研究、物联网安全技术研究、区块链技术在网络安全中的应用研究：

在零信任网络安全模型研究方面，谷歌提出了零信任架构 BeyondCorp 用于内部移动办公、微软提出零信任架构 Azure 并采用人工智能技术有着较多的策略集合、思科提出零信任方案对已有产品进行了考虑对企业员工、工作负载、办公场所等场景进行了相应规划；Belal Ali 等学者[10]在边缘计算中进行了零信任模型规划，强调不信任、验证一切的原则，通过多重身份验证、访问控制等手段提高

企业园区网的安全性。

在物联网安全技术研究方面 Fatima Alwahedi 等学者[11]在物联网安全方面对物联网设备的异构性、广泛的部署和固有的计算限制进行了阐述，阐明了物联网安全的复杂性，同时对包括设备安全、数据传输安全、隐私保护等方面的研究进行了阐明，并使用对物联网安全领域中最先进的基于 ML 的入侵检测系统(IDS)进行了比较分析，揭示了这一动态领域中亟待解决的问题和挑战，并畅想用生成人工智能和大型语言模型增强物联网的安全性。

在区块链技术在网络安全中的应用研究中，国外研究主要关注区块链技术在用户的访问地位认证、大量数据集合性交易（BIG DATA 数据交易）、“零信任”的访问控制等方面，Yanhui Liu 等学者[12]利用区块链不可篡改、不可伪造的特性来加强系统的可靠性。

1.3 本文组织结构

本文主要针对：如何搭建满足企业园区需求的网络基本环境、如何确保企业园区网络安全和应该采用哪些技术及如何在新技术环境下满足企业园区网络安全需要及未来网络安全发展趋势等三个方面进行论述。

主要分为 6 个章节：

第一章 绪论。该章首先介绍了研究背景；其次针对企业园区网安全技术及应用研究的意义进行总体概括，包括企业园区网络搭建及网络安全隐患剖析的路径、企业园区网络安全隐患预防的技术手段、企业园区网络管理及未来技术探究；然后就本文企业园区网络安全技术研究方向上的国内外现状进行总结，最后简述本文总体组织架构。

第二章 企业园区网络安全技术及研究的模拟中所用的关键技术。该章主要对企业园区网络模拟过程中所需的 OSPF、VLAN、VRRP 等技术进行阐述；同时对 VPN、防火墙、入侵检测系统、访问控制等网络安全关键技术进行了论述。

第三章 企业园区网设计。该章分析了企业园区网业务需求、网络管理需求、网络安全需求和拓展性需求形成企业园区典型网络的基本要求。并对典型网络进行初步设计，完成网络设计思想叙述、网络基本设计和总体架构阐述。而且从安全技术要点出发分析安全风险并总结出的安全风险方面设计初步安全方案。

第四章 企业园区网络的模拟器选型及设计实现。本章进行了模拟器的选型及模拟实现，规划出模拟器内设备的接口及对应用途，并配置代码实现联通

第五章 企业园区网基本安全测试。从接入安全、传输安全、数据安全三个方面进行基本的安全测试和安全技术应用。

第六章 未来网络安全技术展望探究及总结。该章对未来网络安全技术进行了探究，同时指出本文尚存在的不足之处及进一步的研究方向。

第 2 章 企业园区网络安全技术及研究的模拟中所用的关键技术

企业园区网络使用关键技术分为两部分进行阐述:第一部分是典型网络模拟使用的相关技术，第二部分是典型网络所使用的关键网络安全技术。第一部分典型网络模拟相关技术，主要从出口区、核心区、汇聚区、接入层四个部分，介绍相关的关键技术。第二部分典型网络所使用的关键网络安全技术从 WAF 技术、IPS 技术、SCAN 技术、内外网相互隔离技术、内网安全技术和反病毒技术等进行论述。

2.1 企业园区网网络模拟技术概述

企业园区网络模拟主要分为：出口区、核心区、汇聚区、接入层四个部分，在技术盖住中将以这四个部分为主要区分介绍相关的关键技术。

（1）出口区

NAT 是 Network Address Translation 这段英文翻译过来的技术名词，在通常过程中我们叫内外网转换，可以根据 IP、端口或 IP+端口的形式进行，有静态 NAT、动态 NAT 和 PAT 这 3 种工作方式。

静态 NAT 就是一对一映射，内部 IP 地址需要和外部进行通信，在配置中多少个内网 IP 地址就要配置多少个外网 IP 地址，不节省珍贵的公网 IP4 的地址，所以一般不用。在使用的时候主要用于服务器，将内网服务映射到外网服务，具体原理如图 2-1 所示。

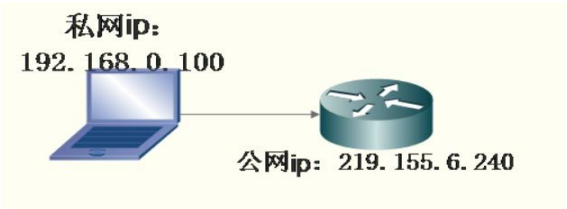


图 2-1 静态 NAT

动态 NAT 是配置外网的公网 IP POOL，当内网 ip 需要访问互联网时候，通过外网的公网 IP POOL 绑定内网 IP，使用结束后释放；其缺点就是，网络不稳定，现今内 IP 的终端访问量很大，所以需要 IP 池，具体原理如图 2-2 所示。

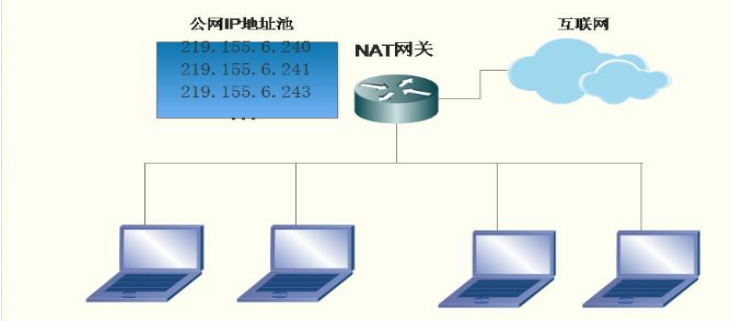
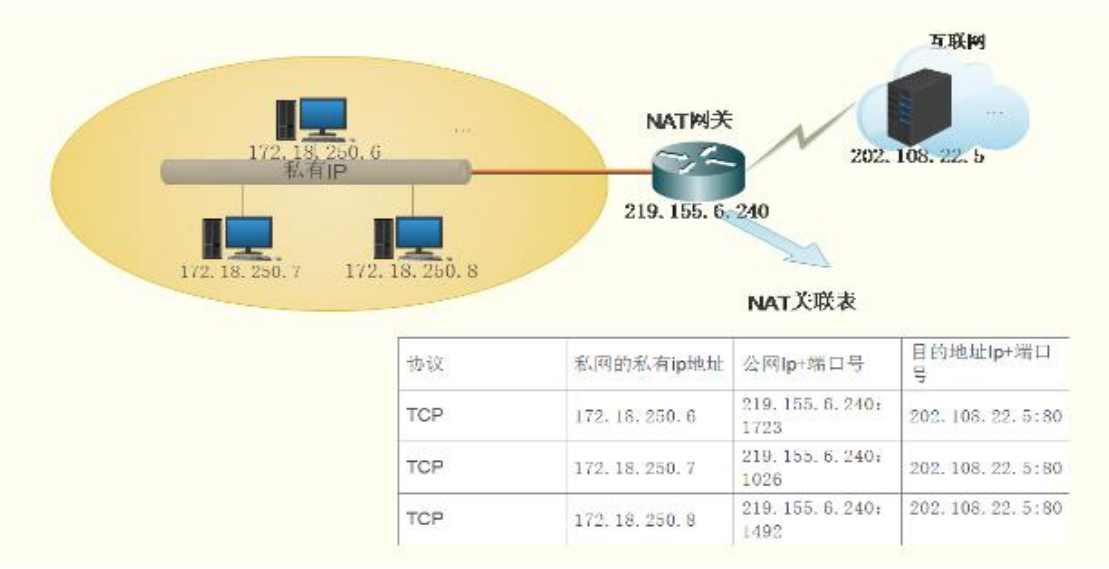


图 2-2 动态 NAT

PAT 让多个内部 IP 映射为一个合法外网公网 IP 地址，使用端口与内部 IP 对应，也就是内外网基于 IP 和端口号之间的转换，具体原理如图 2-3 所示。



协议	私网的私有ip地址	公网ip+端口号	目的地址ip+端口号
TCP	172.18.250.6	219.155.6.240:1723	202.108.22.5:80
TCP	172.18.250.7	219.155.6.240:1026	202.108.22.5:80
TCP	172.18.250.8	219.155.6.240:1492	202.108.22.5:80

图 2-3 PAT

总体来讲，在 NAT 配置过程中可以进行网段隔离来进行数据包伪装，同时也可以进行端口转发将内部网络类似 WEB 等服务进行公网暴露。

（2）核心区

ACL 的英语是:Access Control List,翻译过来是访问控制表，总体来讲，ACL 通过 Permit 和 Deny 语句，进行多条配置形成安全策略，达到控制网络访问的目的，具体原理如图 2-4 所示。

图 2-4 ACL 示意图

VRRP 虚拟网关冗余协议，运行在三层接口上，无论是物理或虚拟模拟的三层接口都能使用该协议，可以使用设备有：三层交换机、路由器、防火墙等。

基本原理是：使用相同的 VRID（虚拟路由器标识符）号的多台协同工作设备通过真实或虚拟接口共同链接，通过选举仅仅一台的 Master 路由器，保持协

议正常工作，只要 Master 路由器不死（可以正常发送 VRRP 存活报文），Backup 路由器无论选举优先级是否很高，都不会抢占 Master 路由器，默默地保持 Backup 状态，直到 Master 路由器死掉。

需要注意的是：互相备份的 VRRP 设备，必须属于同一个 VLAN，VRRP 报文无法正常交互。

（3）汇聚区

DHCP，也叫动态主机配置协议，能够通过 UDP 来开始协议工作。主要是使得各类终端不用配置麻烦的 ip 地址掩码，只用在三层核心层进行 DHCP 配置或者 DHCP 中继就可以使该三层下划分的对应 VLAN 或设备的终端获取 IP 地址。主要作用就是集中管理分配 IP 地址，一般在内网使用，配置 DHCP 要注意终端 IP 在租期结束后可能会变更 IP，具体原理如图 2-5 所示。

图 2-5 DHCP 原理

OSPF 是基于链路状态的动态路由协议。它的主要特点：

1.每个使用 OSPF 的路由器中拥有整个拓扑，但是不传递路由，仅仅发送链路状态通道也就是 LSA 报文。

2.OSPF 有一个非常缓慢的周期更新。

OSPF 基本原理总结为如下过程：

1.发现邻居，建立并维护邻居关系

2.生成 LSA，每台路由器都会生成自己的 LSA

3.泛洪 LSA，使用 OPSF 自身具备可靠传输能力将 LSA 泛洪到区域中的其它路由器上

4.将收到的 LSA 组装成 LSDB，根据 SPF 算法计算出到达拓扑中所有网络的最短路径

5.将计算得出的路由装载到路由表

其具体原理如图 2-6 所示。

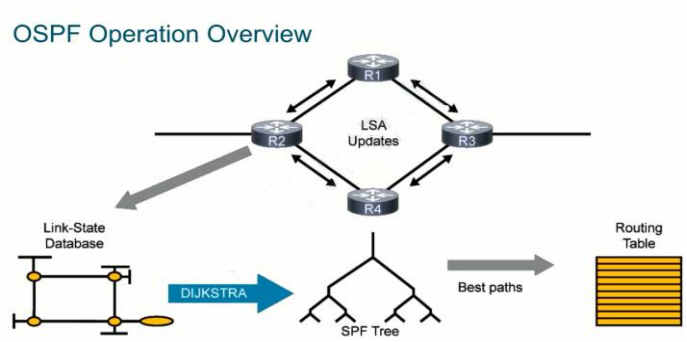


图 2-6 OSPF 原理

链路聚合也称链路聚合协议，也就是 LACP 协议。

作用：

1.整体提升网络的数据吞吐量，解决链路拥塞的问题。

2.把两台设备之间的链路聚集在一块，当做一条逻辑链路使用。

由两种工作模式分别是：动态聚合和静态聚合。

动态聚合：使用 LACP 报文交互，比较灵活。

静态聚合：指定端口进行链路聚合，比较稳定。

生成树技术

STP 生成树：生成树协议主要是解决环路问题（物理、逻辑错误配置），通过 BPDU 报文阻隔冗余链路。

RSTP 快速生成树：升级了，STP 生成树协议选举慢的问题实现快速收敛。

MSTP 多生成树：能够使多棵生成树实现工作。

（4）接入层

VLAN（Virtual LAN），翻译成中文是“虚拟局域网”。LAN 可以是由少数几台家用计算机构成的网络，也可以是数以百计的计算机构成的企业网络。VLAN 所指的 LAN 特指使用路由器分割的网络——也就是广播域。

总结的讲：不同 VLAN 同交换机不能通信，重点是跨交换机 VLAN 通信需进行汇聚链接（Trunk Link）。

2.2 企业园区网中应用的网络安全技术

本文中的企业园区网中应用的网络安全技术，主要从防火墙技术、入侵检测技术、安全扫描技术、内外网隔离技术、内网安全技术和反病毒技术进行论述。

（1）防火墙技术

网络防火墙是一个特殊的网络互联设备，用于加强网络间访问控制，保护内部网络操作环境，限制管理内外部用户访问。作用是控制内部外部网络之间的访

问及数据传送。特点是要配置安全策略进行包过滤。

四种典型结构：多宿主机模式（特点：多块网卡、路由功能禁止、通过应用层代理完成防火墙功能）、屏蔽主机模式（特点：带路由功能、所有内外部链接都放到“堡垒机”、实现网络层安全（包过滤）和应用层安全（代理服务））、屏蔽子网模式（内外部路由器之间放置堡垒主机，减少被侵入影响）、混合模式。

（2）入侵检测（防御）技术

入侵检测技术 IDS，是一个旁路监听设备，原理是将入侵行为进行某种方式编码放入模式库，不停监听和匹配。但是，因为没有主动阻止的功能只能报警，现实应用中被 IPS 取代。IPS，入侵防御系统，在 IDS 被动告警的基础上，进行响应，尝试防止攻击进行主动防御。

具体作用为：

1. 通过匹配模型库对可能存在攻击的网络连接或用户会话将其 Kill；

2. 改变可能存在恶意代码的报文内容，移去或更换恶意代码部分，使其成为良性报文。

（3）安全扫描技术

可以对局域网络、WEB 站点、主机操作系统、系统服务以及防火墙系统的安全漏洞进行扫描，主要是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。扫描技术应具备：信息收集、漏洞检测、弱口令检测等功能。因扫描和骇入流程很像，原理是主要针对系统内核、文件属性、操作系统补丁、病毒等风险文件特征码等进行扫描，对目标主机记录各项主要参数，并进行研判。主要结构是 C/S 结构，现阶段多为云端“大脑”数据匹配模式。

（4）内网安全技术

以数据安全为核心、以身份认证为基础、从信息的源头开始抓安全。主要分为两个部分：移动储存介质管理和网络行为监控。

移动储存介质管理：操作系统内嵌特定程序准入或硬盘及客户端双端加密。

网络行为监控：记录文件操作、控制访问站点、远程登录及下载管理、端口和流量。

数字水印：针对音视频、PDF、WPS、数据库等文件进行重点加密并限制流出主机，仅限军工保密企业使用。

（5）反病毒技术

虽然反病毒和扫描器技术很像，但是因为其危害性单独放出来研究。首先讲病毒这种特殊程序的特征：传染性、未经授权性、隐蔽性、潜伏性、破坏性、不可预见性；其次是传染方式分为：引导型（储存介质引导区）、文件型（独立文件.EXE 等）、混合型；感染方式分为：源码型（编译前插入）、嵌入型（代替

正常程序模块）、外壳型（包裹主程序）和操作系统型（替代服务例如 Svhost）；检测基本方法：外观检测（亮灯、屏幕、串口等）、特征检测（特征代码数据库）、启发式扫描技术（反编译指令序列）。特别是邮件病毒，虽然历史悠久，但是危害长远，主要是附件、WPS（宏病毒）和 ACTIVE 等读写权插件方式进行入侵，在此基础上邮件应用端的云查杀也很重要。

第 3 章 企业园区网设计

该章分为四大部分，第一部分以现在多为东西分部的企业园区架构为例，分析企业园区网业务需求、网络管理需求、网络安全需求和拓展性需求形成企业园区典型网络的基本要求。第二部分对企业园区网络的典型网络进行初步设计，完成网络设计思想叙述、网络基本设计和总体架构阐述。第三部分主要从安全技术要点出发，从接入风险、传输风险、云平台风险、数据风险等方面分析安全风险。第四部分从接入安全、传输安全及审计安全、数据安全设计等方面设计初步方案。

3.1 企业园区网的需求分析

3.1.1 业务需求分析

现阶段我国内基本形成东部研发、西部生产的大型企业模式，主要是东部为分部进行产品研发，西部为总部进行产品生产，同时还有各类业务员全国市场开拓业务。经过长期的调研，本次模拟对企业园区网络的业务进行分析后，总结出的业务需求如表 3-1 所示：

表 3-1 各部门对网络需求分析

部门	主要业务	主要需求	初步网络需求	人员情况
生产部	通过“蓝图”完成产品生产	随时读取研发核心数据	能访问数据中心	主要人员在总部
研发部	设计产品“蓝图”	随时读写研发数据	分部的研发人员能访问数据中心内研发资料	主要人员在分部
业务部	开拓市场	随时读取业务产品资料	可以使用任意联网设备仅读取业务产品资料	全国各地
行政部	内部业务共享办公	访问数据中心共享办公软件	内部网络使用	总部
后勤部（网管）	管理每台接入企业内的网络设备	随时随地管理管控每台网络设备	所有网络设备上“云”且进行流量管控方案解决	总部分部均有
访客	无线接入互联网	仅接入互联网	仅接入互联网	总部

3.1.2 网络管理需求分析

在企业园区进行网络管理过程中，IDC 及各设备都存在于各楼栋业务点内相对应比较分散，对于企业园区的网络安全技术来讲，最重要的便是三个方面：网

络设备是否上线且正常工作、整个企业园区内的局域网是否有异常流量或威胁点、多个业务线能否进行合理运维确保各业务线的业务正常运作。

需要实现的管理功能：远程管理及状态监控包括线路监控、终端监控、协议监控、策略监控、负载监控、分流监控、摄像头监控、交换机监控等，以及流控分流、AC 管理、本地认证服务（外出办公人员）、行为管理、日志管理等。

将网管控制台配置在何处：核心云数据中心或管理人员处。

3.1.3 网络安全需求分析

以本次东西部设置西部生产总部和东部研发分部的大型企业园区为例，安全需求分析需要从网络安全、数据安全、终端安全、物理安全以及应急响应等多个方面进行综合考虑。通过制定针对性的安全策略和措施，可以确保企业园区的网络安全和信息安全，为企业的发展提供有力保障。

本文根据业务需求基础进行安全需求分析，主要分为三个部分进行分析：物理设备安全、传输过程安全、用户权限安全。

物理设备安全中，要根据机房划分管理区域及独立企业园区网络外的门禁，划分人员进入设备间、数据中心及重点区域，防止近源入侵、私自接入。

传输过程安全中，要根据应用、业务及各类需求，尽量选择端对端加密的方式进行数据传输，确保传输过程的数据安全。

在用户权限方面，要重点划分用户、访客以及管理员等权限，以运维举例：管理员-全部权限；DBI-数据库权限；WEB-只能查看权限等。在具体实施过程中：企业的敏感性数据的安全级别：针对各类数据的不同密级进行划分，划定相应网络分布，主要是划分管理 VLAN 及网段隔离广播域，通过细分网络用户的安全级别及其权限：进行各类用户最小权限划分，并严格分组分域。

同时在网络安全需求分析过程中对于各类网络安全设备及网络安全软件的配置和需求也有着重布置。首先是网络设备要满足基本安全功能要求：防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、身份标识和鉴别、加密与数据保护、实时监控与检测等以及最关键的网络安全同意运维，确保事前认证、事中检测、事后溯源；其次在网络是网络安全管理问题，要针对性在邮件、WEB 应用、FTP 或内部 NAS 使用等重点可能出现入侵点的地方对相关使用业务线进行长期教育。

3.1.4 扩展性需求分析

在拓展性需求中分两部分分析，第一部分是云数据中心建设拓展性冗余：在现有情况下，云计算及云数据平台的技术日新月异，带动企业在数据中心建设过程中，要根据技术更新换代的特点，针对性挑选拥有虚拟化的 CPU 搭建相应服务器集群。

第二部分是网络设备建设中，特别是接入点和路由器选取过程中要考虑到物联网时代的影响。在挑选 AP 接入点时候不仅要考虑到 5G 频道速率快的要求，还要有 2.4G 的现有物联网主流接入频段的需求，同时在路由器的挑选过程中要考虑到接入数量的需求，并留下部分 LAN 口供后续进行旁路由操作，若需求暴增或技术更新较快则选择侵入式旁路由配置将主要流量放在旁路由中分担主路由压力，若部分业务增加则选择非侵入式在客户端配置网关。

3.2 企业园区网的网络设计

（1）企业园区网的规划设计思想

本文企业园区网络的设计理念旨在满足大多数企业的各类不同业务需求，因此选择构造典型的大型企业园区网络，接下来将从网络架构、网络设备（简述）、网络带宽、网络安全、灵活性与拓展性等方面进行构造，下面是企业园区网络模拟设计中的基本设计思想及设计理念：

网络架构：设计合理的网络架构，包括核心层、汇聚层和接入层，确保网络的高效性和稳定性。在实际设计过程中，分为东部研发分部和西部生产总部进行，通过搭建 VPN 实现内部网络互通互联。

网络设备：选择高性能、高可靠性的网络设备，如交换机、路由器、防火墙等，以满足园区网络的各项需求。同时，根据现今国内 2027 年前完成网络设备及终端国产化的需求，所有设备能采用国产化设备均进行国产化设备模拟。在本次典型网络设计中，出口区路由器采用国产 Ikuai 软路由进行，其余核心区及接入区的网络设备通过华为二层、三层交换机实现，需要注意的是软路由内集成防火墙、VPN 网关、AC 服务等设备功能。

网络带宽：根据园区的业务需求和人员数量，合理规划网络带宽，确保网络的高速传输和顺畅访问。因现阶段网络的普及，各类设施设备包括物联网设备、视觉检测产品设备等所需网络带宽大，因此在接入层和核心去采用链路聚合复用。

网络安全：设计完善的安全策略，包括网络隔离、访问控制、数据加密等措施，以保障园区网络的安全。特别是在设计中采用 DMZ 区，将 WEB、邮件、协同办公等服务，部署中将集成到云数据中心区域，同时根据核心交换机的数据镜像进行数据交换在云数据中心处加装蜜罐、DLP 系统、堡垒机网管审计等措施保证服务安全稳定。

（2）网络结构设计

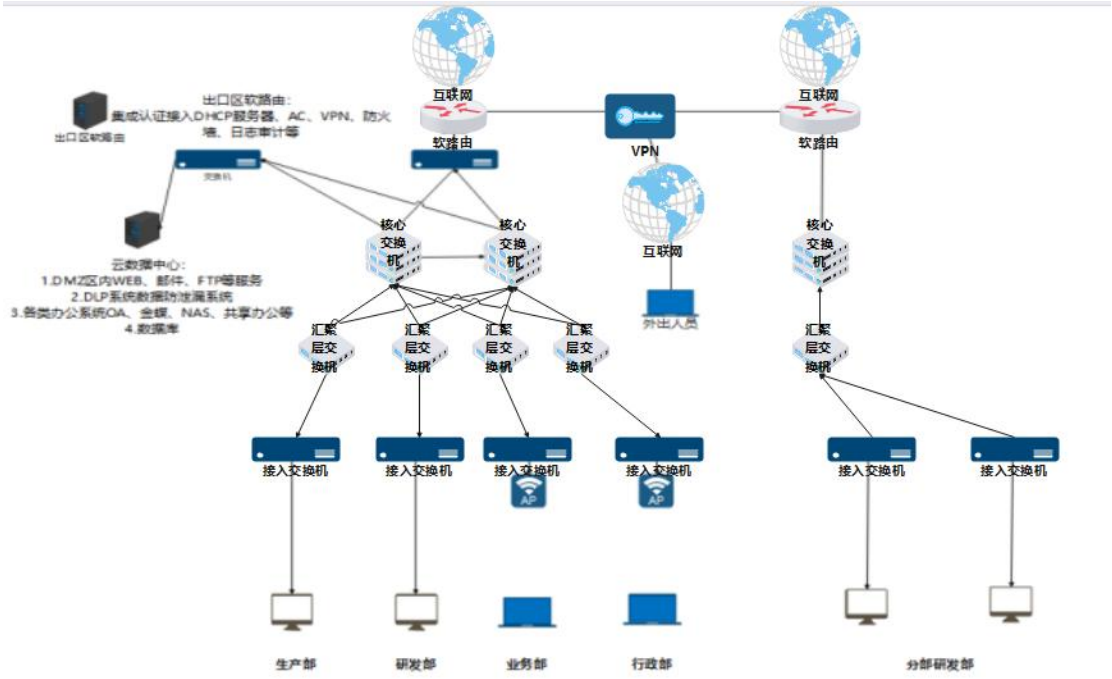


图 3-1 网络总体架构图

根据企业的实际情况，网络采用三层结构。简述各层的作用，为接下来的组网方案规划设计提供理论基础，其基本架构如图 3-1 所示。

（1）核心层。接入软路由后的分线器下，配置两台高速三层交换机进行 DHCP 中继、两台高速三层交换机互相备份并链路聚合。

（2）汇聚层。四台三层交换机，设置 VLAN 分割广播域、基于 VLAN 配置接入层终端网关，并配置多生成树解决环路问题。

（3）接入层。4 台二层交换机，在这里需要配置 do1tq 和 qinq 两种 VLAN 封包模式，前者主要解决总部内网划分 VLAN、后者解决外网传输后 VLAN 的可使用性，主要是研发部可以跨三层基于 VLAN 进行广播域分割。

（4）出口区。由软路由进行模拟接入互联网，软路由内有：DHCP 服务、VPN 服务器端客户端认证服务、PPPOB 拨号上网服务、流量监控及防火墙、WAC 服务器端及云端集成 SNMP 协议能进行远程管控分布在各地的路由器和核心交换机服务。使用软路由的原因：主要是内存、储存及日志容量和服务终端数量能够基于服务器的性能随时增长，并且根据需要随时进行所有配置备份，发生意外情况，分钟内可以重新部署。同时，根据未来各企业配置“大模型”的巨量带宽需求，软路由可以通过集合多 WAN 口来解决扩容麻烦及各品牌路由器兼容的问题。

软路由内对应的一般物理设备架构为路由器、防火墙（包括防火墙内的 VPN 网关功能）、流量控制审计设备、AC 服务端，主要是通过集成网络内主干设备及网络安全的关键功能在软路由内，在遇到突发安全风险事件时可以通过虚拟设备回滚恢复网络或通过虚拟平台迅速重新部署网络，软路由内的物理架构模拟如图 3-2 所示。

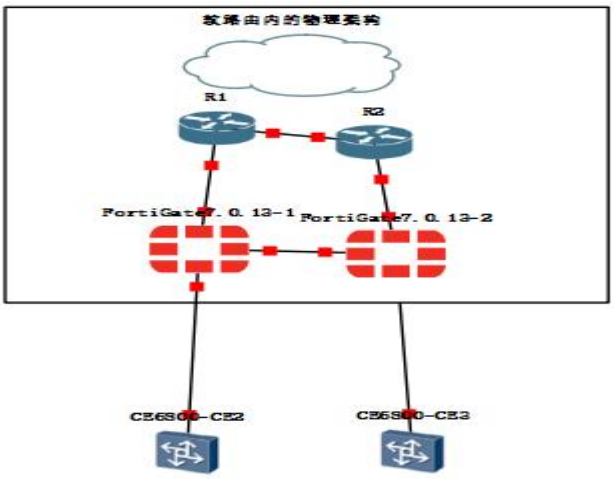


图 3-2 出口区软路由内对应物理架构

（3）网络节点设计

本次模拟的网络节点设计主要针对生产部、研发部、业务部、行政部、后勤部（网管）这我五个主要部门的网络需求划分 VLAN 及关键设备网段。

其中生产部主要人员在总部，需要随时访问数据中心获取技术“生产资料”，通过数据中心内协同办公软件进行报表上传，但是不需要访问财务、业务数据因此对其广播域设计为仅访问数据中心。

研发部主要人员在分部，需要随时访问数据中心内的 Jenkins、Gitlab 等代码仓库及 Mysql、SQL server 等数据库和 NAS 等文件库进行设计工作，因数据中心属于内网所以需要进行 VPN 链接内网使用，VPN 设计搭建在软路由之间，VPN 服务端网关搭建在总部软路由内，其广播域域设计因特殊性应仅限制其访问云数据中心。

业务部主要人员在全国各地均有分部，因此在对其设计是通过互联网访问 VPN 网关进行内网业务数据、产品资料访问，广播域仅限访问云数据中心。

行政部所有人员均在总部，需要访问云数据中心通过 OA、金蝶、协同办公等软件功能进行企业内部管理，包括人员、客户、财务信息的管理。

后勤部主要人员在总部和分部都有分部，主要是网管运维的作用，需要在总部分部都能访问云数据中心进行运维同时对全企业网络的管理都能随时随地展开。

访客仅限在总部访问网络，主要接入形式限制为 AP 的 wifi 接入，包括部门内私人网络设备的使用也规划在访客区域，确保企业内部网络安全，部门的网段和 VLAN 具体设计如表 3-2 所示。

表 3-2 部门网段及 VLAN 广播域设计表

用 途	VLAN ID	CIDR	DHCP	可访问 VLAN
出口区 总部软路由	默认	192.168.22.0/24	OFF	ALL
生产部	10	192.168.1.0/24	ON	10、60
研发部	20	192.168.2.0/24	ON	20、60
业务部	30	192.168.3.0/24	ON	30、60
行政部	40	192.168.4.0/24	ON	40、60
访客（AC）	50	192.168.50.0/24	ON	50
云数据中心	60	192.168.60.0/24	ON	60
后勤部（网管）	66	192.168.66.0/24	ON	ALL

3.3 企业园区网安全风险分析

（1）接入风险

主要是终端及接入层面临的网络协议相关的安全风险。企业物联网灯开关、智能电器、门禁系统等无线连接设备。例如 802.11 协议的“WIFI 断网漏洞”还没有修复，通过该协议漏洞可以使得该无线路由器下的所有设备断网，其它类似的漏洞也由很多。同时，接入风险中也要重点考虑近源攻击，在主要数据存储和应用部署的云数据中心要重点进行的人员管理管控，防止访客私自接入核心层及以上设备造成网络协议的漏洞利用。

（2）传输风险

现阶段企业使用的 VPN，拥有暴漏公网 IP 导致业务面暴漏的风险。如图所示，在进行全网 VPN 服务扫描中会暴漏业务面，在运维没能及时更新设备漏洞或新 0day 被发现的情况下，会导致内部网络数据泄露，通过资产扫描器对公网暴露服务扫描可以发现很多 VPN 的服务 IP 都有被攻击的隐患，具体情况如图 3-3 所示。

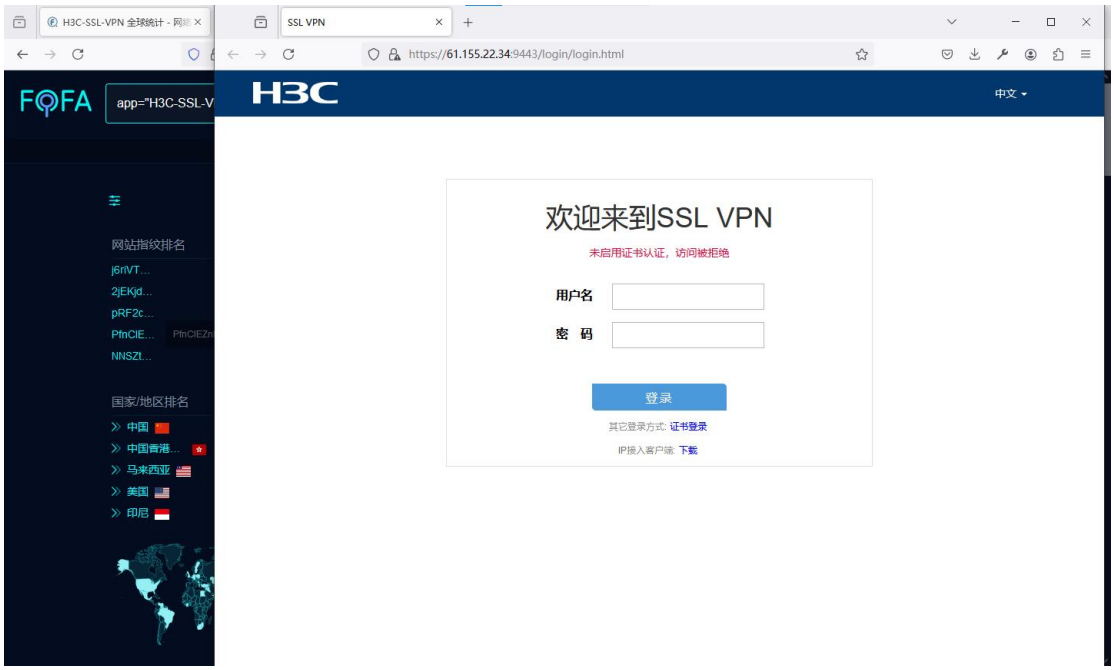


图 3-3 VPN 业务面风险扫描

（3）云平台风险

云计算平台服务安全威胁：目前云计算平台的操作系统例如主流的 OpenStack 和 VMwareEXSI 等都存在未知漏洞，攻击者有可能通过虚拟机漏洞攻击而获取云平台的管理员权限。

云平台风险还有一部分风险是在利用共享技术漏洞进行的攻击上，其原理是：由于云租户是多租户共享，如果云租户之间的隔离措施失效，一个云租户有可能入侵另一个云租户的环境，或者干扰其他云租户应用系统的运行。特别是在使用 Docker 等资源过程中内部 Docker 网络配置互访情况下，在 Docker 中又配置 Racher 等云平台管理平台，Docker 内部网等其他原因导致非授权访问，在现如今中间件群完全虚拟化的大背景下就会导致整体业务面暴漏。

（4）数据风险

数据安全风险包括采集、传输、处理、储存、交换和销毁多个方面，作为企业园区网安全多个方面都有涉及，但在本文中主要在处理、储存、交换三个方向进行分析风险。在数据处理中，需要警惕计算和展示过程中的数据泄露；在数据储存中，需要警惕共享、访问控制中的越权访问；在数据交换中，警惕导入导出的数据风险隐患特别是载体或传输路径的安全。

3.4 企业园区网初步安全方案

（1）接入安全

物理环境安全：交换机处进行门禁、监控等举措确保设备安全。

准入和访问控制：通过 ACL 策略及流量监控实现应用级别的接入控制。

交换机安全协议启用：DHCP Snopping、ospf authentication-mode hmac-md5（端对端的接口加盟认证）、绑定 MAC

传输安全:接入层和汇聚层设备间基于端对端伪线仿真通过 VPN 等端对端加密隧道的方式确保传输通道安全防止监听。

审计安全：在可以部署日志的地方都进行日志部署管理，重点在网络出口设置网络管理系统、数据中心部署堡垒机；从事前、事中、事后进行全流程管理，确保可以预防、监控、取证。

（2）数据安全

首先解决数据储存、处理、交换的数据安全问题：

在数据安全的数据存储中，要根据数据存储系统的安全、数据机密性、访问控制、容灾备份、日志审计、存储期限进行相应管理。

在数据安全的网络数据交换中，要进行数据库安全基线、访问配置、数据存储加密（分级加密）、特权账号管理、行为日志审计等工作；在数据机密性方面至少要使用安全的加密算法对敏感信息进行加密存储;在访问控制中要对数据库访问控制权限、特权账户、高敏操作进行重点配置；在容灾备份中采用多云/异地数据备份设置备份频率定时进行全量备份。

在数据处理的安全隐患排除中要重点对计算、展示两个方面进行，主要进行脱敏、日志记录、权限和访问控制和数据分析处理过程安全。本文中主要重点在实现日志记录搭建和用户级网络权限及访问控制。

其次从用户角度上进行数据安全管理：

远程用户：在云数据中心、总部分部边界处部署防护墙并提供 SSLVPN 服务确保端对端数据安全。

本地用户：内部设备绑定 MAC 且专机专用，严格管控外联，对于个人电子设备按照访客 ACL 策略管理。

总体方案：针对性的敏感数据采用含有数字水印的 DLP 系统进行加密，通过 DLP 系统划分管理区域，同时对特别重要文件在使用水印技术时进行时间设置;在屏幕等外显设备上加入肉眼不可见的屏幕水印管控敏感信息方便事后溯源。

第 4 章 企业园区网络的模拟器选型及设计实现

4.1 企业园区网络模拟器选型

现阶段主流的网络模拟器有 GNS3 模拟器、eNSP 模拟器、Cisco Packet Tracer 以及 EVE-NG 模拟器。

GNS3 模拟器：GNS3 是一款图形化界面的网络虚拟软件，支持多平台运行（Windows、Linux、MacOS 等）。它稳定高效，使用简单，能够模拟思科路由的大部分内容以及交换机的部分功能。

eNSP 是由华为提供的免费、可扩展、图形化操作的网络仿真工具平台。它主要针对网络路由器、交换机进行软件仿真，支持大型网络模拟。

Cisco Packet Tracer：Cisco Packet Tracer 是一款网络设计和配置的教学工具，支持用户设计、构建和模拟计算机网络。它提供可视化的编程环境，对网络设备进行配置，并实时显示数据包在网络中的传输过程。

EVE-NG：EVE-NG 是一款基于开源技术的网络虚拟化平台，主要用于构建和管理复杂的网络拓扑。它支持模拟各种主流厂商的设备，如路由器、交换机、防火墙等，使得用户能够在虚拟环境中搭建真实的网络架构

综合考虑，eNSP 仅仅支持华为设备、CPT 仅支持思科设备考虑选型为 GNS3 及 EVE-NG，两款模拟器都支持华为、思科等多款路由器和交换机镜像且支持 Docker 及 VMware 网络互联及山石、绿盟等厂商的多款网络安全设备模拟。经过选型，虽然 EVE-NG 能够支持近似于物理机的模拟效果，从路由器、交换机的基本启动开始就进行模拟，但 EVE-NG 的模拟过程中镜像启动慢及占用内存过大，资源占用高。从这个方面考虑选型模拟器为 GNS3。

4.2 企业园区网络关键架构模拟

4.2.1 总体架构

企业园区网络模拟中总体分为四大板块:总部板块、分部板块、云数据中心及外部互联。在模拟过程中采用 VMware(虚拟机)的容器模拟软路由（Ikuai）、云数据中心，VMware（虚拟机）的网络 VMnet0 进行桥接互联网模拟真实网络环境并进行云数据中心的相关应用部署。因本次网络需使用 VMnet 网络进行真实网络模拟，其中软路由内的网卡和模拟物理高速三层交换机和二层交换机的服务器的网卡都将通过 VMware 进行虚拟化模拟，特别是云数据中心的 NAT 地址转换为方便模拟也将通过 VMnet 的技术进行模拟联通。

现将在模拟过程中 VMnet 网络及各网段的作用网络进行设计，参数如表 4-1 所示，状态如图 4-1 所示。

表 4-1 VMware 网络配置及网关设置

VMnet 的编号	作用的网络	IP 网段	网关
VMnet0	物理网络路由 WAN 口	10.0.0.0/24	10.0.0.1（现实物理机）
VMnet2	总部网络 LAN 口	192.168.22.0/24	192.168.22.1
VMnet3	分部网络 LAN 口	192.168.33.0/24	192.168.33.1
VMnet4	渗透测试入口	192.168.55.0/24	192.168.55.1
VMnet8	配置软路由 VMware 内应用预留 WEB 口	192.168.23.0/24	192.168.23.1
注：VMnet1	GNS3 服务器端	192.168.88.0/24	192.168.88.1

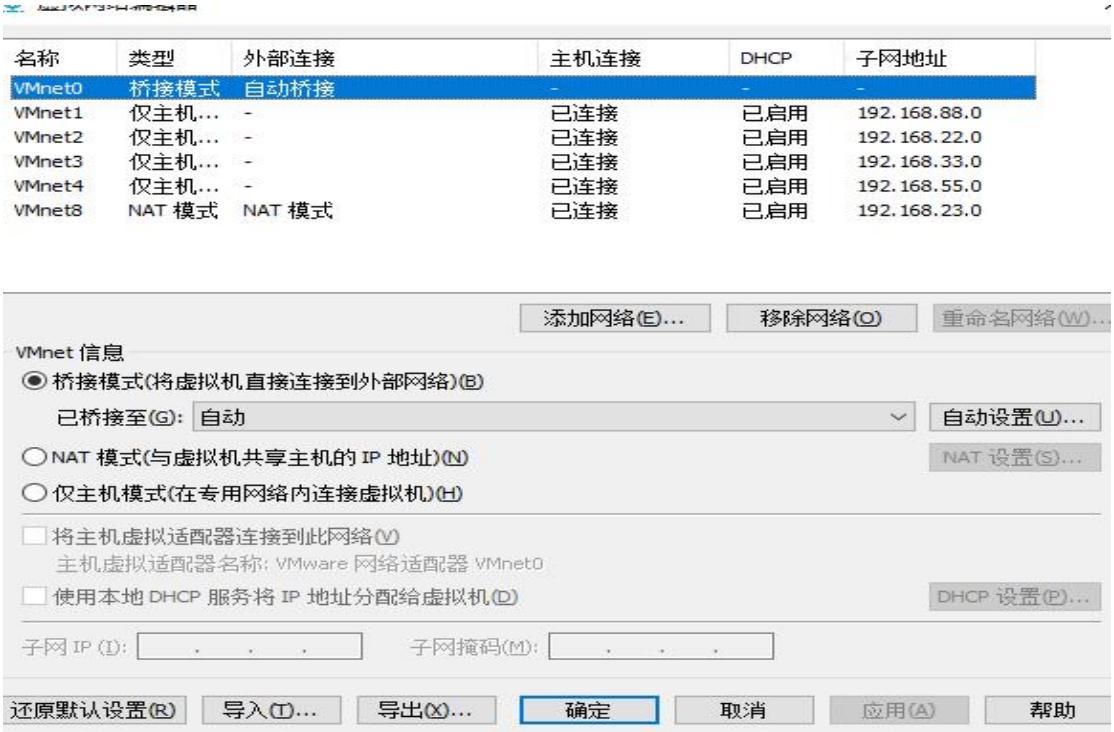


图 4-1 VMware 网络编辑器

在 GNS3 的总体模拟中需要使用 5 块网卡，分别进行总部分部软路由使用，还有物理网络（互联网）的模拟以及 GNS3 服务器和云数据中心使用的 NAT，参数如表 4-2 所示，状态如图 4-2 所示。

表 4-2 VMware 网络配置及网关设置

网卡编号	作用的网络	模拟作用
Eth0	GNS3 默认	传输设备信息
Eth1	GNS3 默认	传输设备信息
Eth2	桥接互联网	模拟器内设备连接互联网
Eth3	总部软路由 LAN 口	模拟器内设备连接软路由
Eth4	分部部软路由 LAN 口	模拟器内设备连接软路由
Eth5	渗透测试网口	渗透入口

图 4-2GNS3 的网卡配置

企业园区的总体模拟图分为四大板块，总部、分部、互联、云数据中心，具体架构，具体情况如图 4-3 所示。

其中总部和分部板块出口区：由软路由进行防火墙、DHCP、VPN、AC 等服务模拟。WAN 口接入实际互联网，LAN 口接入总部、分部核心层。

出口区软路由：WAN 口上网方式通过 DHCP 获取物理路由器 IP 地址进行连接互联网，LAN1 口绑定 VMWARE 内 NAT 网卡方便主机访问暴露 WEB 控制地址 192.168.23.0/24（总部：192.168.23.33/24 分部：192.168.23.34/24），内配置 PPPOE 拨号上网、VPN 认证双端（C/S）。

总部核心层：总部的软路由后接入核心层两台 CE6800 的华为高速三层交换机做 DHCP 中继、VLAN 网关配置、链路聚合、双机备份等服务模拟,。

总部汇聚层：核心层后接入四台 CE6800 华为多端口高稳定性三层交换机为汇聚层，用于获取核心层数据镜像进行安全保护措施及各类内网服务和 DMZ 区设置。

分部核心层（汇聚层）：分部软路由后跟 CE6800 华为三层高速交换机做核心层（汇聚层）功用，因规划中分部不做研发数据储存，所有数据上“总部数据中心”云储存，所以主要保证分部传输安全和接入安全即可。分部核心层（汇聚层）后直接接入二层交换机进行终端接入工作。

数据中心：在模拟中通过搭建 Docker 来模拟虚拟化的工作；通过 Jumpserver 堡垒机等来模拟 IPS、审计等网络安全设备；通过云数据中心来模拟 WEB、邮件、FTP 等服务

外部访问主机：通过 WIN 平台集成 WSL 版本的 Kali、VPN 客户端等组成，主要由两个功用：一是进行 VPN 端连通性测试，模拟业务部外出员工通过互联网进行内网业务产品资料访问；二是方便模拟过程中的安全测试。

具体模拟设备选择 CE6800 华为交换机为核心、汇聚层主要设备，连接及配置如表 4-3，核心设备配置代码见表后。

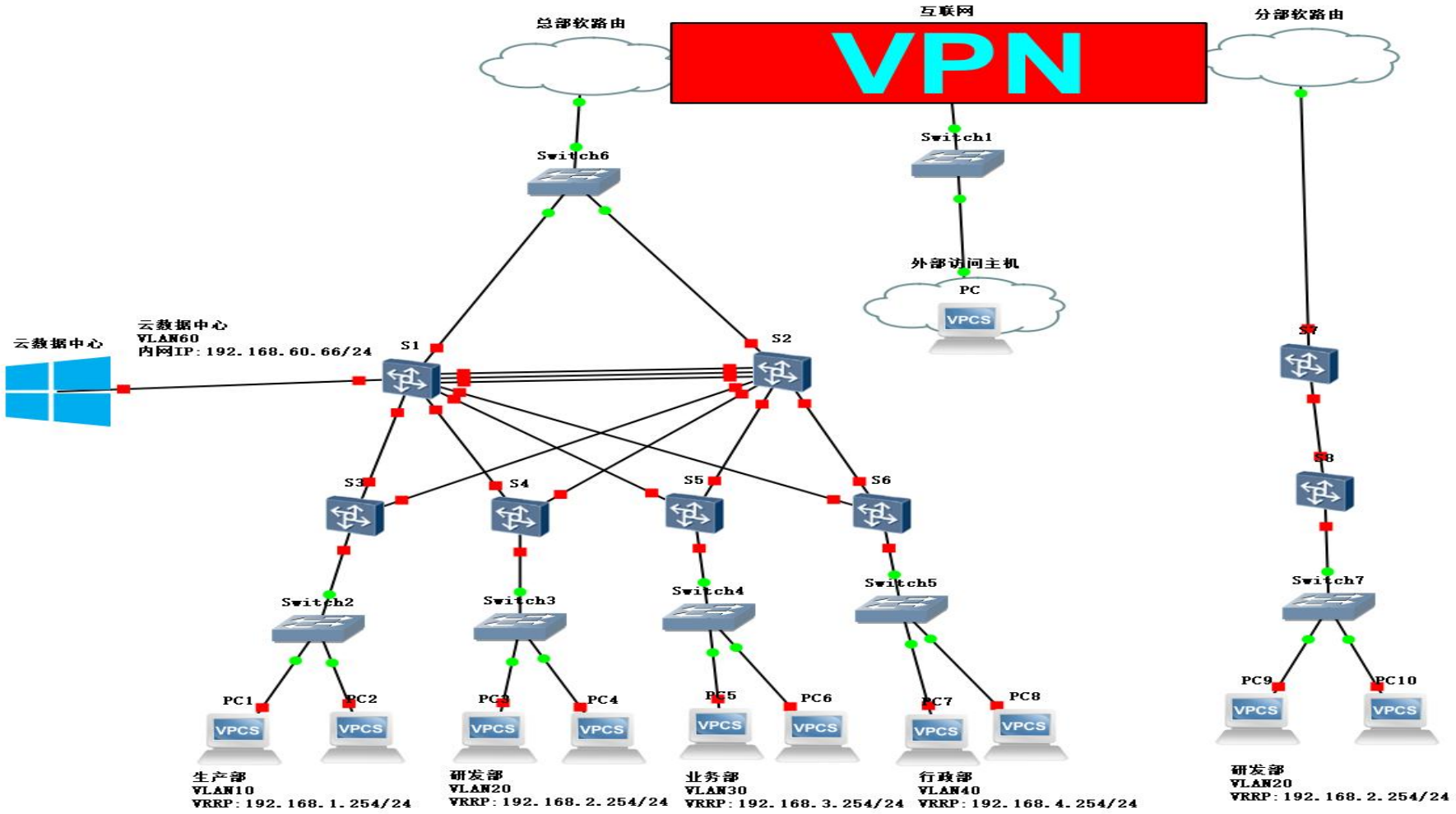


图 4-3 企业园区的总体模拟图

表 4-3 各模拟设备网络 IP 地址及接口分配表

设备	接口	对方接口	模式/VLAN	用途
S1	G1/0/1	S2 G1/0/3	Eth-Trunk	链路聚合
	G1/0/2	S2 G1/0/2	Eth-Trunk	链路聚合
	G1/0/3	S2 G1/0/1	Eth-Trunk	链路聚合
	G1/0/4	R1 G0/0/0	Access VLANIF100 （192.168.22.2）	通过 VLANIF100 接入总部软路由
	G1/0/5	S3 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/6	S4 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/7	S5 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/8	S6 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/9	云数据 中心	Trunk	允许经过的 VLAN 范围为所有
S2	G1/0/1	S1 G1/0/3	Eth-Trunk	链路聚合
	G1/0/2	S1 G1/0/2	Eth-Trunk	链路聚合
	G1/0/3	S1 G1/0/1	Eth-Trunk	链路聚合
	G1/0/4	R1 G0/0/0	Access VLANIF100 （192.168.22.2）	通过 VLANIF100 接入总部软路由
	G1/0/5	S3 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/6	S4 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/7	S5 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/8	S6 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
软路由	ETH3	G1/0/0	192.168.22.1	总部软路由和核心三层互通
	ETH4	G1/0/0	192.168.33.1	分部软路由和核心三层互通
	ETH5	G1/0/0		外部访问互联网
S3	G1/0/1	S1 G1/0/5	Trunk	允许经过的 VLAN 范围为所有
	G1/0/2	S2 G1/0/5	Trunk	允许经过的 VLAN 范围为所有

设备	接口	对方接口	模式/VLAN	用途
	G1/0/3	二层 交换机		接入终端
S4	G1/0/1	S1 G1/0/6	Trunk	允许经过的 VLAN 范围为所有
	G1/0/2	S2 G1/0/6	Trunk	允许经过的 VLAN 范围为所有
	G1/0/3	二层 交换机		接入终端
S5	G1/0/1	S1 G1/0/7	Trunk	允许经过的 VLAN 范围为所有
	G1/0/2	S2 G1/0/7	Trunk	允许经过的 VLAN 范围为所有
	G1/0/3	二层 交换机		接入终端
S6	G1/0/1	S1 G1/0/8	Trunk	允许经过的 VLAN 范围为所有
	G1/0/2	S2 G1/0/8	Trunk	允许经过的 VLAN 范围为所有
	G1/0/3	二层交换 机		接入终端
S7	G1/0/0	Eth4	Access VLANIF200 （192.168.33.2）	通过 VLANIF200 接入分部软路由
	G1/0/1	S8 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
S8	G1/0/1	S7 G1/0/1	Trunk	允许经过的 VLAN 范围为所有
	G1/0/10	二层 交换机		接入终端

1)核心层核心三层交换机 S1 核心配置代码：

```
sysname S1 // 设置设备名称为 S1
vlan batch 10 20 30 40 60 100 // 创建 VLAN 批量，并指定 VLAN ID
stp instance 1 root primary // STP1 将该设备设为主根桥
stp instance 2 root secondary // STP2 中将该设备设为次根桥
dhcp enable // 启用 DHCP 服务
stp region-configuration // 配置 STP 区域
region-name yb-test // 设置区域名称为 yb-test
instance 1 vlan 10 20 // 在 STP 实例 1 中将 VLAN 10 和 20 纳入该区域
```

instance 2 vlan 30 40 // 在 STP 实例 2 中将 VLAN 30 和 40 纳入该区域
active region-configuration // 激活 STP 区域配置
interface Vlanif10 // 配置 VLAN 接口 10
ip address 192.168.1.1 255.255.255.0 // 设置 IP 地址和子网掩码
vrrp vrid 1 virtual-ip 192.168.1.254 // 配置 VRRP 虚拟路由器 ID 为 1，虚拟 IP
vrrp vrid 1 priority 120 // 设置 VRRP 虚拟路由器优先级为 120
dhcp select relay // 使用全局 DHCP 中继
DHCP relay gateway 192.168.22.254// DHCP 中继服务 ip 地址
interface Vlanif20
ip address 192.168.2.1 255.255.255.0
vrrp vrid 2 virtual-ip 192.168.2.254
vrrp vrid 2 priority 120
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif30
ip address 192.168.3.1 255.255.255.0
vrrp vrid 3 virtual-ip 192.168.3.254
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif40
ip address 192.168.4.1 255.255.255.0
vrrp vrid 4 virtual-ip 192.168.4.254
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif100
ip address 192.168.22.2 255.255.255.0
interface Vlanif60
ip address 192.168.60.254 255.255.255.0
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Eth-Trunk1 // 配置以太网链路聚合接口 Eth-Trunk1
port link-type Trunk // 设置为 Trunk 链路类型
port Trunk allow-pass vlan all // 允许经过的 VLAN 范围为所有
interface G1/0/1 // 配置 G1/0/1 接口

eth-Trunk 1 // 将接口加入到 Eth-Trunk1 链路聚合组
interface G1/0/2 // 配置 G1/0/2 接口
eth-Trunk 1 // 将接口加入到 Eth-Trunk1 链路聚合组
interface G1/0/3 // 配置 G1/0/3 接口
eth-Trunk 1 // 将接口加入到 Eth-Trunk1 链路聚合组
interface G1/0/4 // 配置 G1/0/4 接口
port link-type access // 设置为 Access 链路类型
port default vlan 100 // 设置默认 VLAN 为 100
interface G1/0/5 // 配置 G1/0/5 接口
port link-type Trunk // 设置为 Trunk 链路类型
port Trunk allow-pass vlan all // 允许经过的 VLAN 范围为所有
interface G1/0/6 // 配置 G1/0/6 接口
port link-type Trunk // 设置为 Trunk 链路类型
port Trunk allow-pass vlan all // 允许经过的 VLAN 范围为所有
interface G1/0/7 // 配置 G1/0/7 接口
port link-type Trunk // 设置为 Trunk 链路类型
port Trunk allow-pass vlan all // 允许经过的 VLAN 范围为所有
interface G1/0/8 // 配置 G1/0/8 接口
port link-type Trunk // 设置为 Trunk 链路类型
port Trunk allow-pass vlan all // 允许经过的 VLAN 范围为所有
interface GigabitEthernet1/0/9 // 配置 GigabitEthernet0/0/9 接口
port link-type access // 设置为 Access 链路类型
port default vlan 60 // 设置默认 VLAN 为 60

2)核心层核心三层交换机 S2 核心配置代码：

sysname S2
vlan batch 10 20 30 40 100
stp instance 1 root secondary
stp instance 2 root primary
dhcp enable
stp region-configuration
region-name yb-test
instance 1 vlan 10 20
instance 2 vlan 30 40
active region-configuration

interface Vlanif10
ip address 192.168.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.1.254
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif20
ip address 192.168.2.2 255.255.255.0
vrrp vrid 2 virtual-ip 192.168.2.254
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif30
ip address 192.168.3.2 255.255.255.0
vrrp vrid 3 virtual-ip 192.168.3.254
vrrp vrid 3 priority 120
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif40
ip address 192.168.4.2 255.255.255.0
vrrp vrid 4 virtual-ip 192.168.4.254
vrrp vrid 4 priority 120
dhcp select relay
DHCP relay gateway 192.168.22.254
interface Vlanif100
ip address 192.168.22.2 255.255.255.0
e-Trunk 1
interface Eth-Trunk1
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/1
eth-Trunk 1
interface G1/0/2
eth-Trunk 1
interface G1/0/3
eth-Trunk 1

```
interface G1/0/4
port link-type access
port default vlan 100
interface G1/0/5
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/6
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/7
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/8
port link-type Trunk
port Trunk allow-pass vlan all
```

3)汇聚层交换机 S3 核心配置代码：

```
sysname S3
vlan batch 10 20 30 40
stp region-configuration
region-name yb-tset
instance 1 vlan 10 20
instance 2 vlan 30 40
active region-configuration
interface G1/0/1
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/2
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/3
port link-type access
port default vlan 10
```

4)汇聚层交换机 S4 核心配置代码：

```
sysname S4
```

```
vlan batch 10 20 30 40
stp instance 1 root secondary
stp instance 2 root secondary
stp region-configuration
region-name yb-tset
instance 1 vlan 10 20
instance 2 vlan 30 40
active region-configuration
interface G1/0/1
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/2
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/3
port link-type access
port default vlan 20
```

5)汇聚层交换机 S5 核心配置代码：

```
sysname S5
vlan batch 10 20 30 40
stp region-configuration
region-name yb-tset
instance 1 vlan 10 20
instance 2 vlan 30 40
active region-configuration
interface G1/0/1
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/2
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/3
port link-type access
port default vlan 30
```

6)汇聚层交换机 S6 核心配置代码：

```
sysname S6
vlan batch 10 20 30 40
stp instance 1 root secondary
stp instance 2 root secondary
stp region-configuration
region-name yb-tset
instance 1 vlan 10 20
instance 2 vlan 30 40
active region-configuration
interface G1/0/1
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/2
port link-type Trunk
port Trunk allow-pass vlan all
interface G1/0/3
port link-type access
port default vlan 40
interface Ethernet0/0/4
port link-type access
port default vlan 40
```

7)分部核心层三层交换机 S7 核心配置代码：

```
sysname S7 //  设置设备名称为 S1
vlan batch 20 200
interface G1/0/0
port link-type access
port default vlan 200
interface Vlanif200
ip address 192.168.33.2 255.255.255.0
interface Vlanif20
ip address 192.168.2.254 255.255.255.0
dhcp select relay
DHCP relay gateway 192.168.33.1
```

interface G1/0/1

port link-type Trunk

port Trunk allow-pass vlan all

8)汇聚层交换机 S8 核心配置代码：

sysname S8

vlan batch 10 20 30 40

interface G1/0/0

port link-type Trunk

port Trunk allow-pass vlan all

interface G1/0/1

port link-type access

port default vlan 20

4.2.2 总部板块网络模拟测试情况

MSTP 验证：通过 S1 和 S3 的 STP 查询命令 DISPLAY STP 查看 STP 的工作状态。CIST Bridge、握手包等 STP 状态的验证结果如图 4-4 所示。

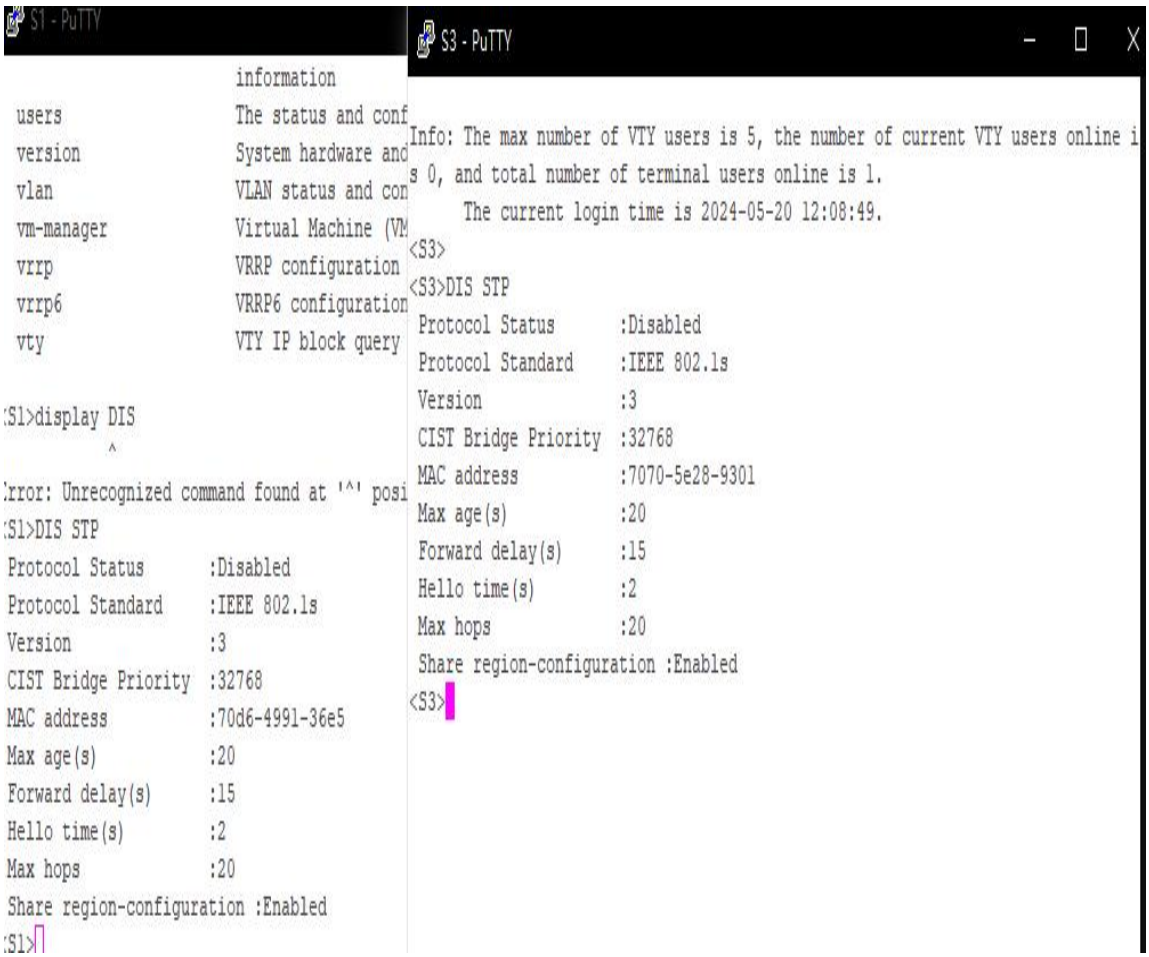


图 4-4 MST 验证

DHCP 验证：本地机（模拟主机）通过 VMware 网卡访问 DHCP，可以通过查询本机 DHCP 服务验证模拟网络内的 DHCP 服务是否启动，验证结果如图 4-5 所示。

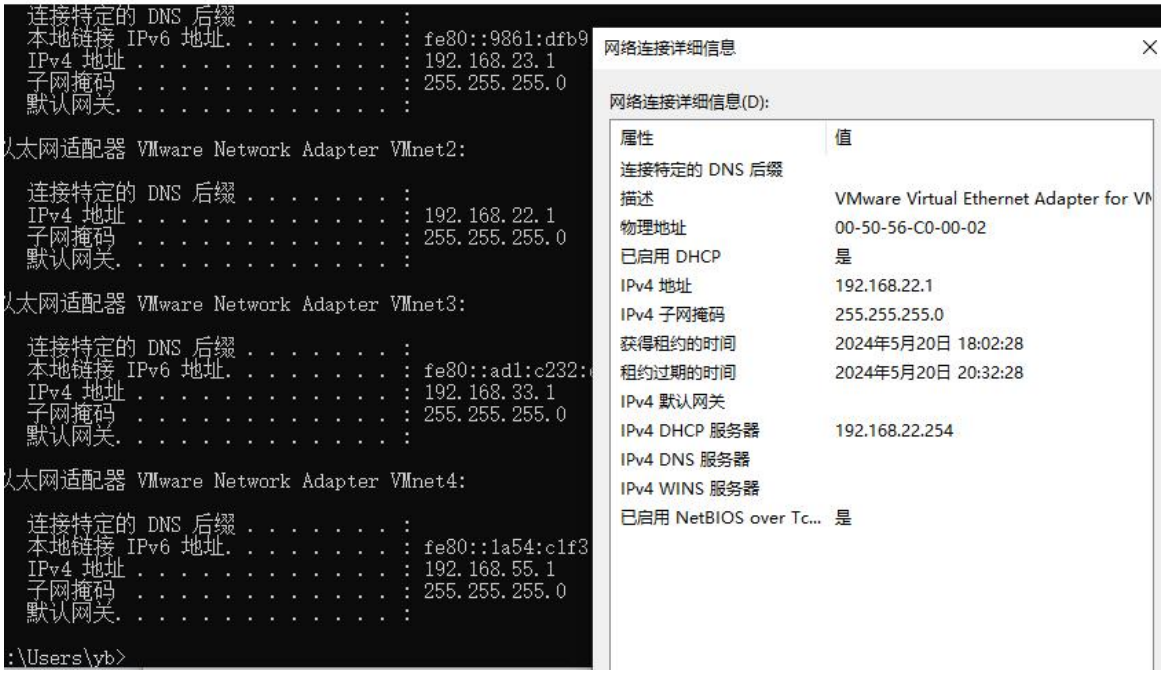


图 4-5 DHCP 验证

VRRP 验证:通过在 S1 和 S2 中用 DIS VRRP 命令查询 VRRP 服务工作情况，验证结果如图 4-6 所示。

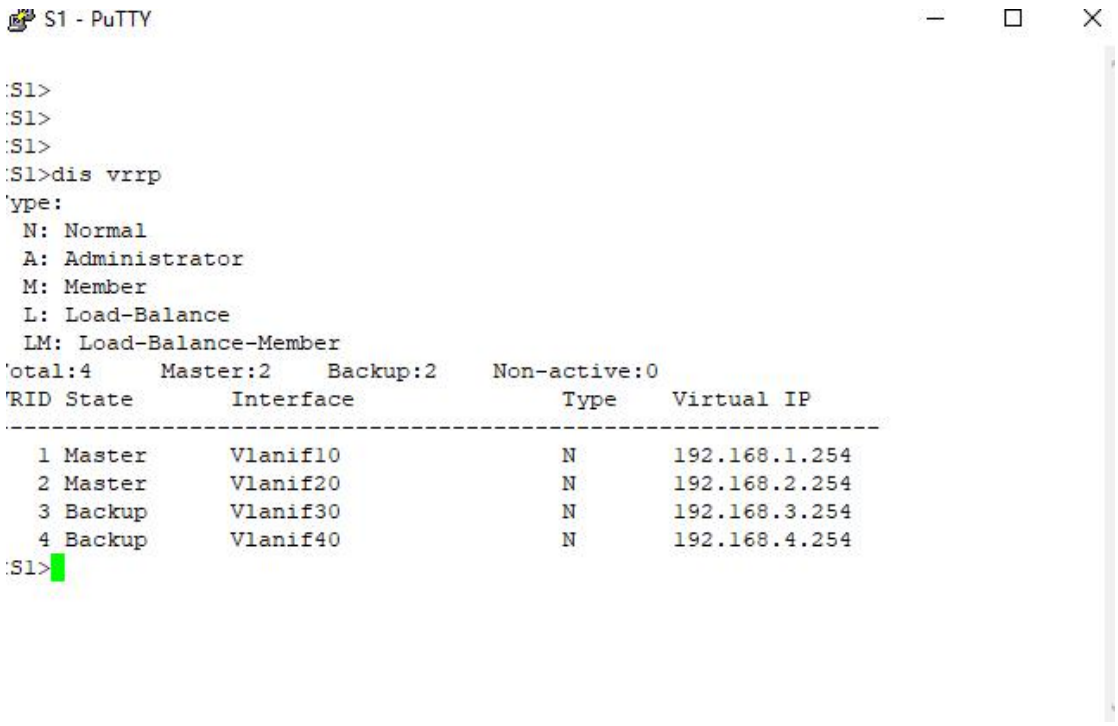


图 4-6 VRRP 验证

LACP 验证：通过在 S1 或 S2 内用 DIS ETH-TR 1 查看链路聚合情况，验证结果如图 4-7 所示。

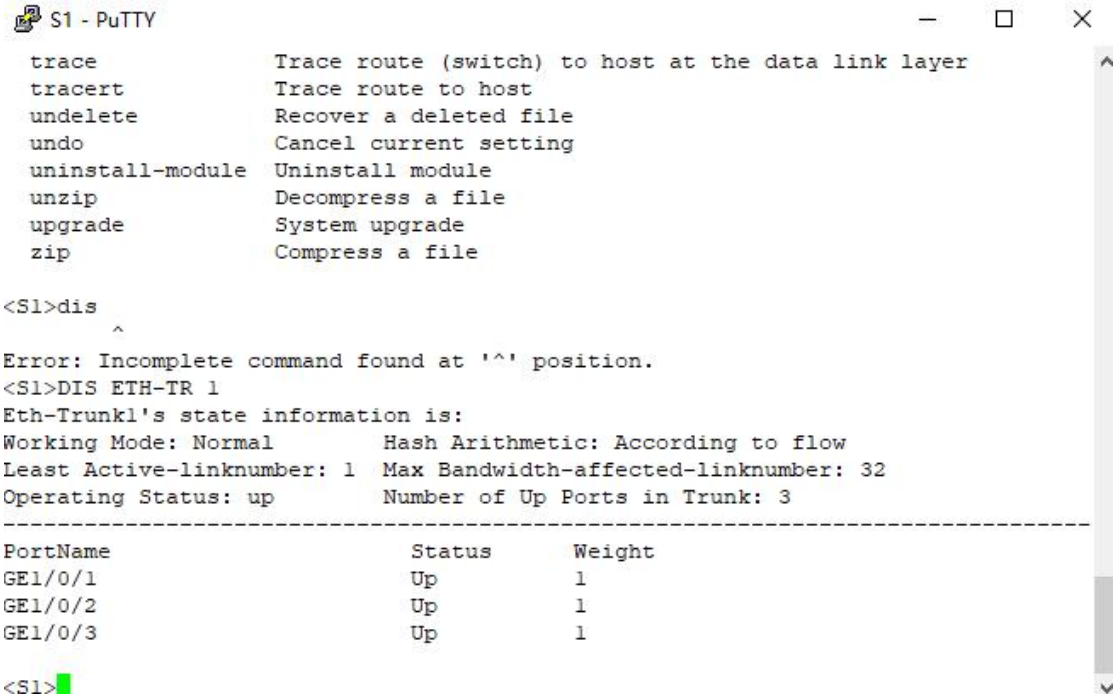


图 4-7 链路聚合验证

4.2.3 分部板块网络模拟测试情况

VPN 验证：分部板块的 VPN 客户端是通过总部软路由配置 OPENVPN 服务器端实施内网互通的。本次测试 VPN 功用通过外出人员主机连接 VPN 测试 192.168.22.1（总部软路由对接核心层 IP）的连通性证明 VPN 功能可用性。验证结果如图 5-8 所示。

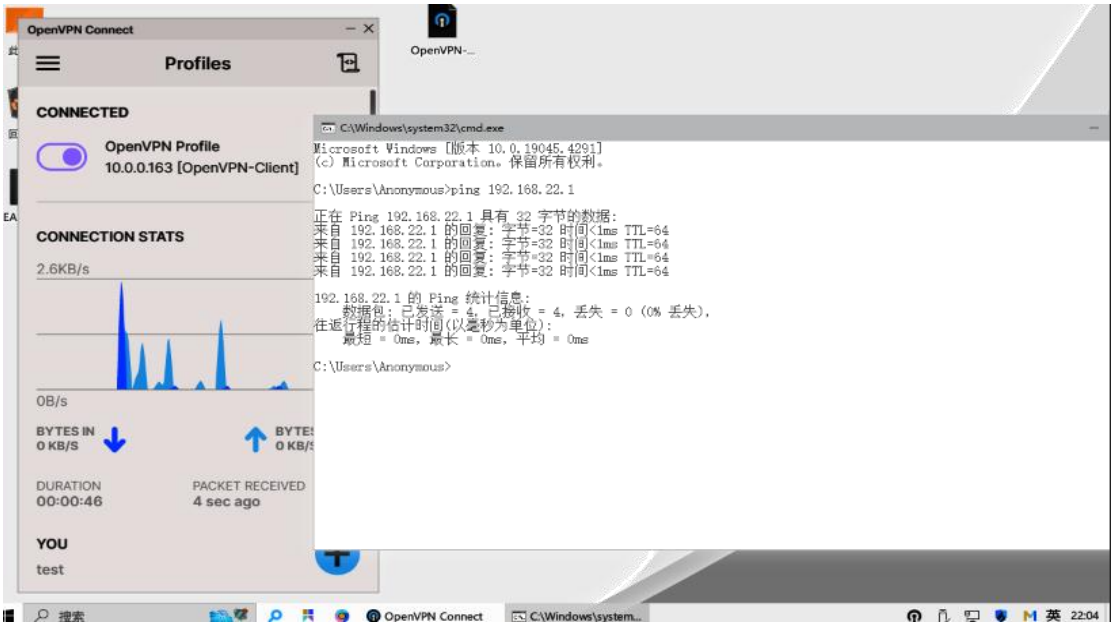


图 4-8 VPN 功能验证

DHCP 验证：本地机（模拟主机）通过 VMWARE 网卡访问 DHCP，可以通过查询本机 DHCP 服务验证模拟网络内的 DHCP 服务是否启动，分部 DHCP 功能验证如图 4-9 所示。

图 4-9 分部 DHCP 验证

4.2.4 云数据中心模拟测试情况

虚拟环境验证：通过配置 Docker 容器群可以迅速部署 HIfish 蜜罐、堡垒机、DLP 系统等安全措施。通过客户机登录云数据中心 SSH，验证 Docker 来进行虚拟环境验证，确保后续配置进行，容器验证结果如图 4-10 所示。

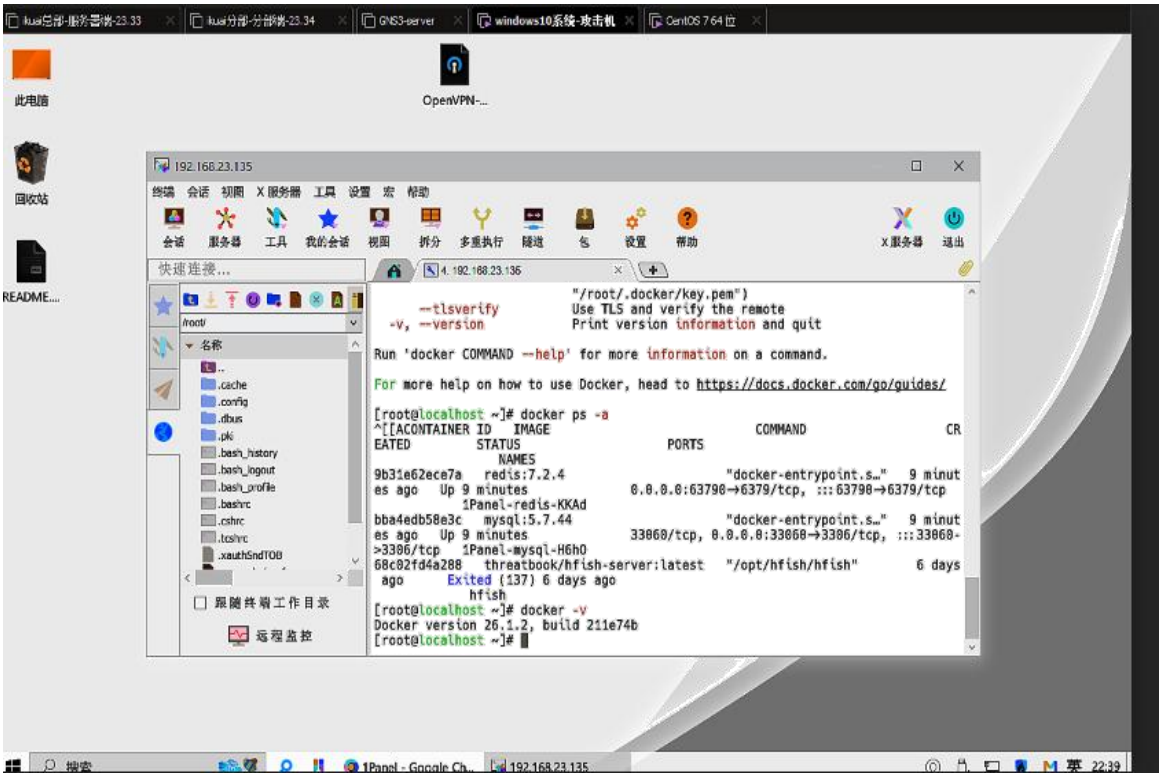


图 4-10 虚拟环境验证

云数据中心基本功能验证：数据中心是协同办公、NAS、研发数据储存等的企业内部办公的基础，本次模拟通过 NAS 访问验证协同办公基本功能，验证结果如图 4-11 所示。

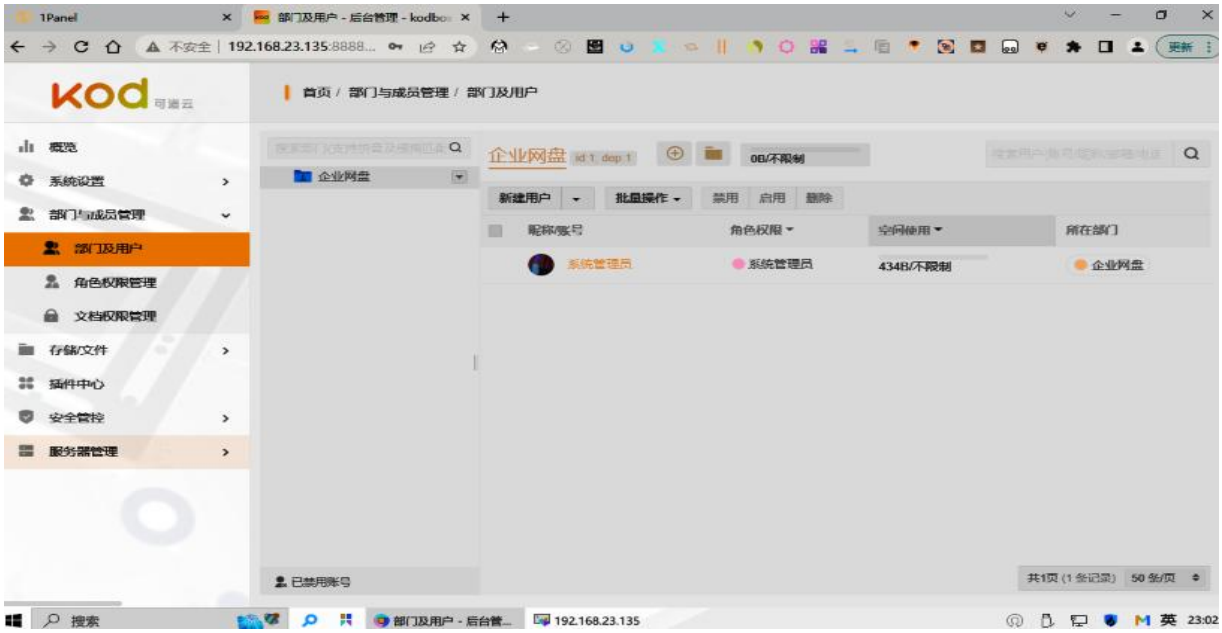


图 4-11 云数据中心基本功能验证

第 5 章 企业园区网基本安全测试

本章主要进行网络安全测试，针对网络协议方向进行渗透测试，主要分接入安全、传输安全及审计安全和数据安全。

5.1 接入安全测试

接入安全，本文测试主要一网络协议缺陷测试为住，主要挑选三个个重点安全测试进行：分别是生成树欺骗、DHCP 劫持、ARP 攻击。

5.1.1 生成树欺骗及应对举措

根据企业典型网络设计来看，SW1-SW2 两台核心三层交换机和 SW5 二层交换机，组成了一个“窃听”风险区，如图 5-1 所示。

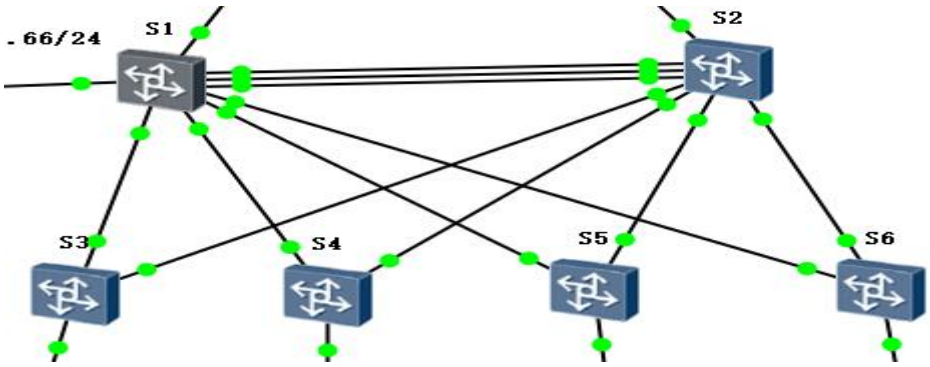


图 5-1 生成树区域

其“窃听”原理如下：

1. 理论依据：选举银桥（网桥的 ID=优先级+MAC 地址），同等优先级下，mac 地址小的优先级大。

2. 实施过程：构造“虚拟或假的”交换机，设置 STP 模式，通过 STP PRIORITY 0 类似命令将银桥优先级提为最高，并且通过 MAC 模拟技术迫使“虚拟或假的”交换机成为主根，促成部分备份链路封堵，进而以主根形式抓包收集信息。

解决方案：启用 BPDU 保护；原理：在边缘主机连接端口配置 BPDU 保护后，接收到 BPDU 的收敛报文时，立即封堵边缘主机端口。

5.1.2 DHCP 劫持及应对举措

根据企业典型网络设计来看，R1 为内网 DHCP 分配服务器，当入侵主机接入 SW1 或 SW2 内后就可以模拟 DHCP 服务器、DNS 服务器，其危害性能导致客户机使用假的网络配置进而进行“中间人攻击”导致主机断网、主机信息窃取等危害。在本次模拟中的影响区域如图 5-2 所示。

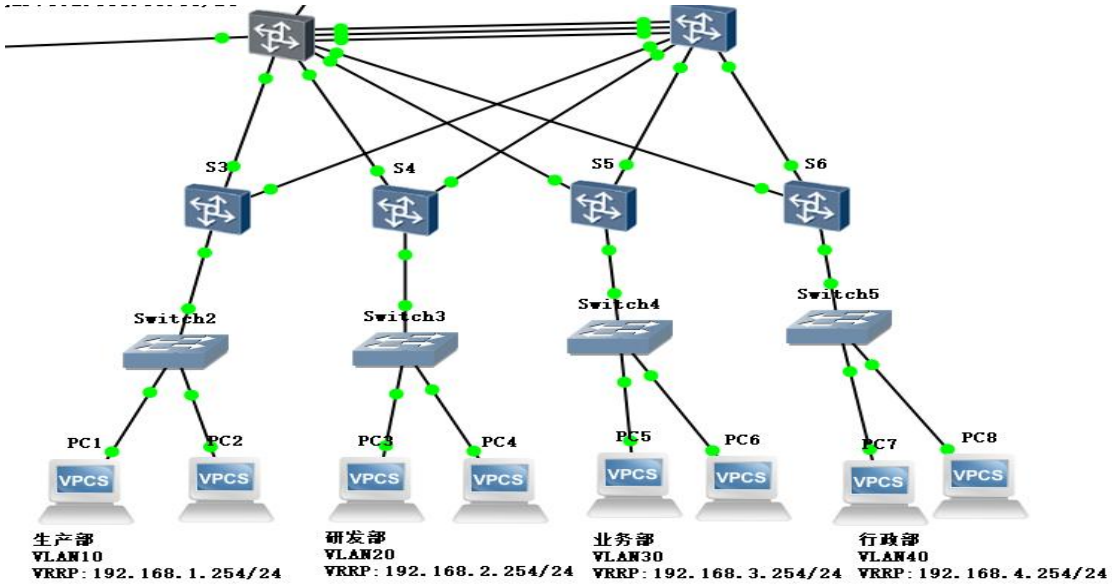


图 5-2 DHCP 影响区域

“中间人攻击”的理论依据：DHCP 中继速度比本地 DHCP 速度满，内网局域内主机会优先选择速度快的内网渗透 DHCP 服务器而不是 DHCP 中继单播的服务器。

实施过程：构造相同 DHCP 服务器配置，交换机，设置相同网段的 DHCP 服务器。

解决方案：使用 DHCP Snooping 技术，进行监控和验证，防止被攻击。

5.1.3 ARP 攻击及应对举措

现分为两种形式：主机型，通过更改同网络内其他在线主机 IP 欺骗路由器；路由器型，通过更改为路由器网关欺骗其他在线主机。本机模拟的部分 ARP 表如图 5-3 所示。

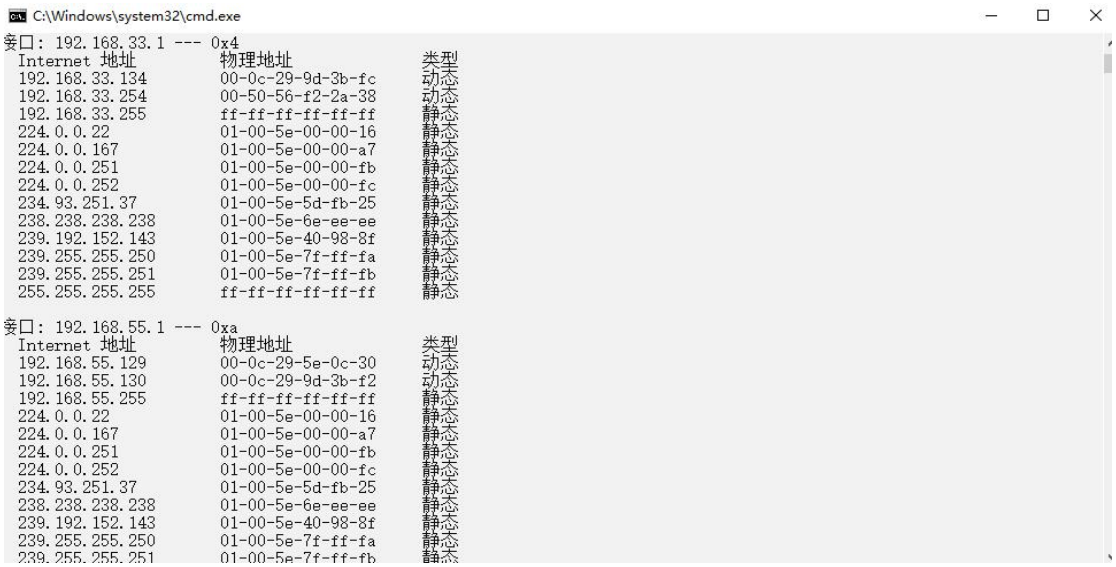


图 5-3 ARP 表

理论依据：局域网内主机基于 MAC 通信，ARP 负责当“翻译官”，本次攻击测试主要是替代“翻译官”的角色。

实施过程：通过 IP ADD 命令更改同局域网内地址。

解决方案：通过 user-bind static ip-address 192.168.1.1 mac-address AB:CD:EF:GH:XX 命令绑定网关和 MAC 地址，通过 arp anti-attack rate-limit enable 命令配置 DAI 动态 ARP 检测。

5.2 传输安全及审计安全测试

5.2.1 传输安全

本次传输安全测试主要通过抓包 VMnet2 和 VMnet3 网卡进行，因 VMnet2 和 VMnet3 直接配备了 OPENVPN 链接，因此传输明文 user 和 power 查看是否由明文，即可证明传输数据的安全性。图 5-4 为路由器内置 WIRESHARK 抓包，用于验证明文和密文区别、图 5-5 为 VPN 服务器端配置页面。其中测试过程中的 lan2 接口为软路由对接到 GNS3 网络设备模拟端的接口，因此在抓包过程中只要筛选出从数据中心到客户端的数据包就能对比出 VPN 的作用是否体现。在具体配置中，VPN 的验证通过软路由的账户管理系统进行认证方便管理各类人员和及时封堵危险外联。

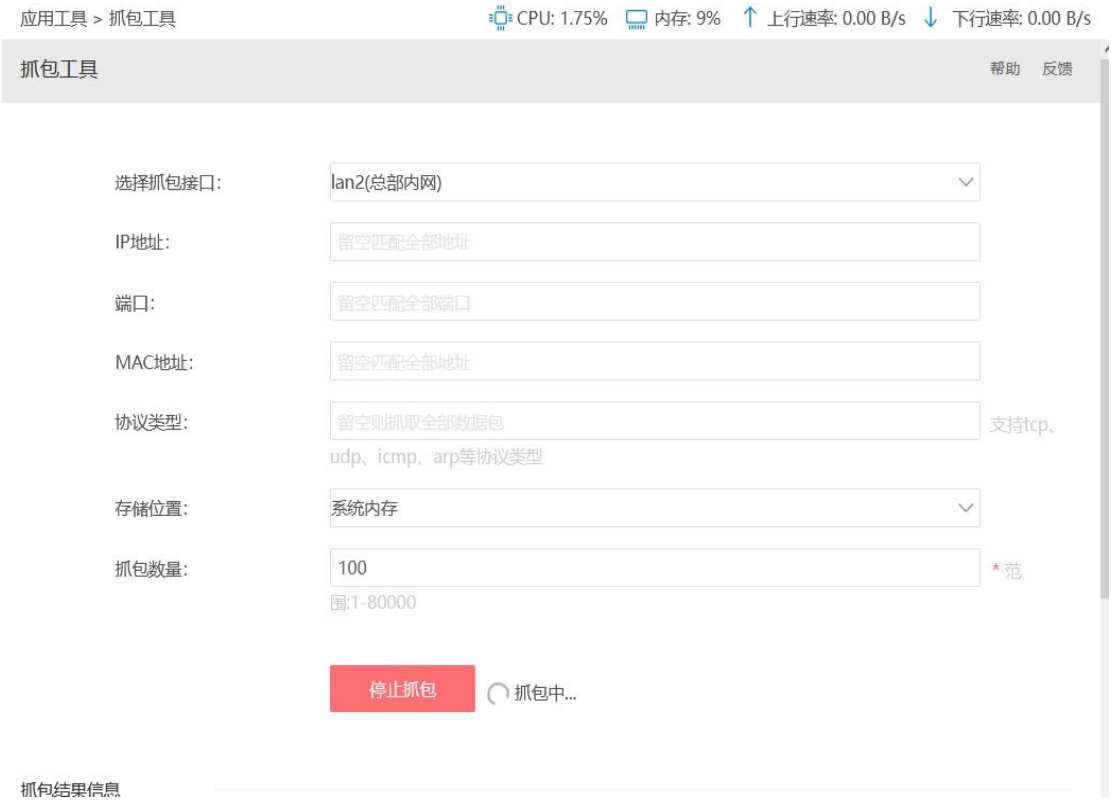


图 5-4 抓包

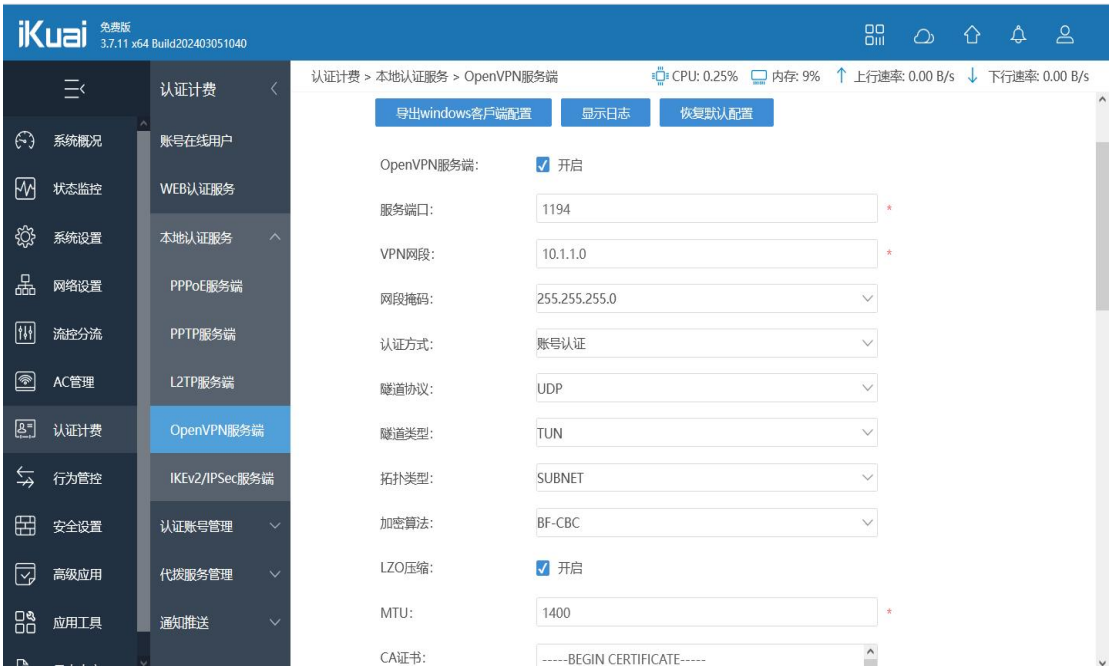


图 5-5 VPN 服务端配置

5.2.2 审计安全测试

本次审计安全测试，通过日志的审查进行，现阶段典型网络的日志有访问日志及系统日志，图 5-6 为访问日志，图 5-7 为系统日志。

图 5-6 访问日志

图 5-7 系统日志

5.3 数据安全测试

数字水印等技术在数据安全中，虽然很重要，但是市面上很难找到相应模拟器。因此，数据安全测试主要进行数据备份功能测试。

备份功能主要通过磁盘本地快照进行数据时序化可回滚，通过阿里云 OSS 等云储存或 SFTP 等私有 NAS 储存进行数据备份。

通过验证虚拟环境快照、定时上传配置文件到阿里云 OSS、NAS、SFTP 服务器等云存储终端来验证数据安全是否能达到：保护数据的完整性、可用性和安全性的重要意义。本次模拟通过部署在云数据中心内的 NAS 进行数据备份，内网地址为：192.168.23.135:8888。图 5-8 展示虚拟化快照，图 5-9 展示多储存设备定时容灾热存储。

图 5-8 快照

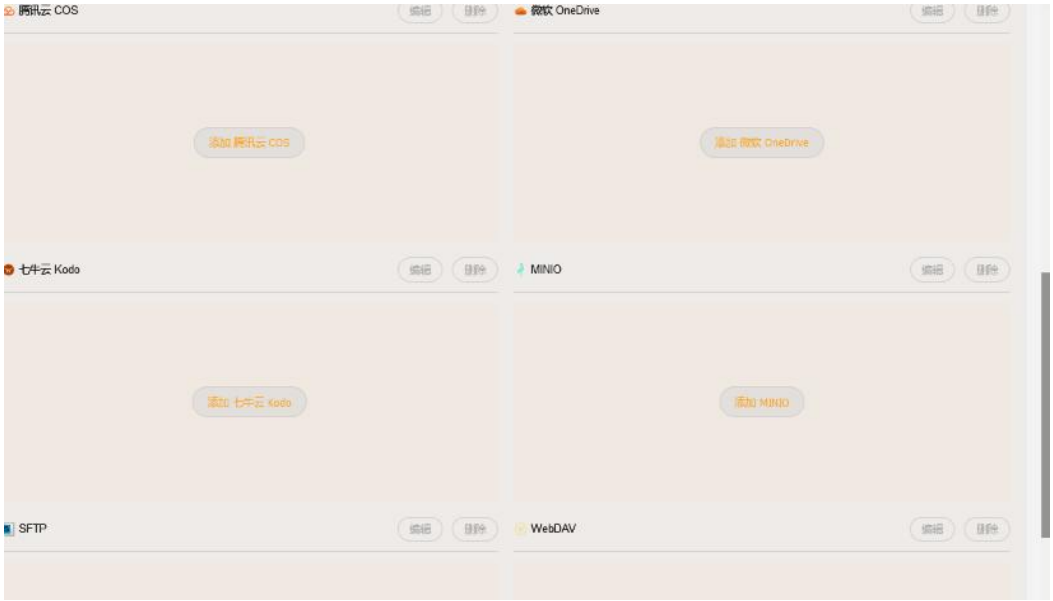


图 5-9 多容器储存备份

5.4 企业园区网网络安全应用功能部署

在一般的企业园区网的网络安全应用中有蜜罐、堡垒机等各类举措，本次主要挑选蜜罐（含态势感知）和堡垒机的应用功能部署进行，同时为了模拟真实运维环境，本次模拟中还将通过 FRP 技术将部署在内网（云数据中心）IP 为 192.168.23.135 的安全应用映射到公网 IP 为 65.154.145.96 云服务器中，其中部署安全应用的端口号+安全入口，如表 5-1 所示。

表 5-1 网络安全应用对应端口

应用	接口	对接对象	内网 ip 及端口	外网展示 ip 及端口	满足需求
蜜罐	G1/0/1	核心交换机 S1、S2	https://192.168.23.135:4433/web/	https://65.154.145.96:4433/web/	风险感知威胁阻隔
堡垒机	G1/0/1	核心交换机 S1、S2	http://192.168.23.135:80	http://165.154.145.96:80	各业务连接
云服务平台内网	G1/0/1	核心交换机 S1、S2	http://192.168.23.135:2333/ybtest	无	Docker 容器管理、linux 性能可视化、FRP 服务端、数据库
云服务平台外网	互联网	互联网	无	http://165.154.145.96:12755/e220ee98c9/	Docker 容器管理、linux 性能可视化、FRP 客户端
NAS	互联网	互联网	192.168.23.135:8888	http://65.154.145.96:8888/	共享办公、云存储
FRP 服务器端	互联网	互联网	无	http://165.154.145.96:7500	内网穿透
FRP 客户端	G1/0/1	互联网	http://192.168.23.135:7400	无	内网穿透

5.4.1 蜜罐系统测试

主要是通过主动暴露本次模拟中容易被攻击 Telnet、Linux 服务器 web 管理端（宝塔）、WEBVPN 服务（思科）、若依管理系统（JAVA 开发模板）、防火墙（绿盟）、邮件服务、Ikuai（路由）等服务，来使得保护真正数据和业务的安全。具体配置模板详情如图 5-10 所示。

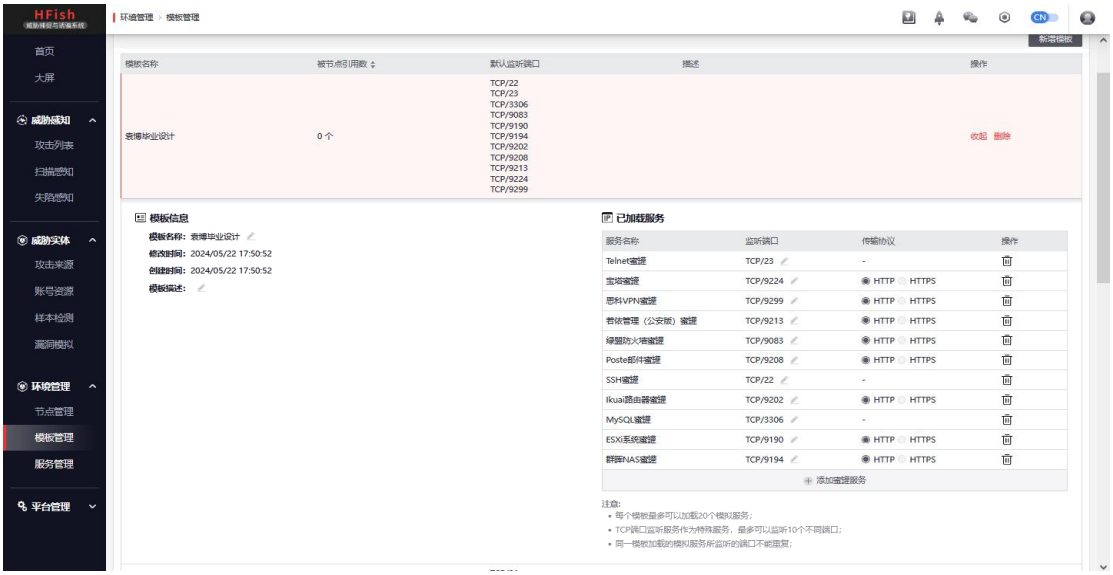


图 5-10 蜜罐系统

测试：已经知道现阶段公网通过 FRP 穿透模拟真实外网的暴露 ip 为 165.154.145.96，为了方便通过云扫描来模拟攻击，我们将把内网服务映射公网，FRP 映射概述如图 5-11。

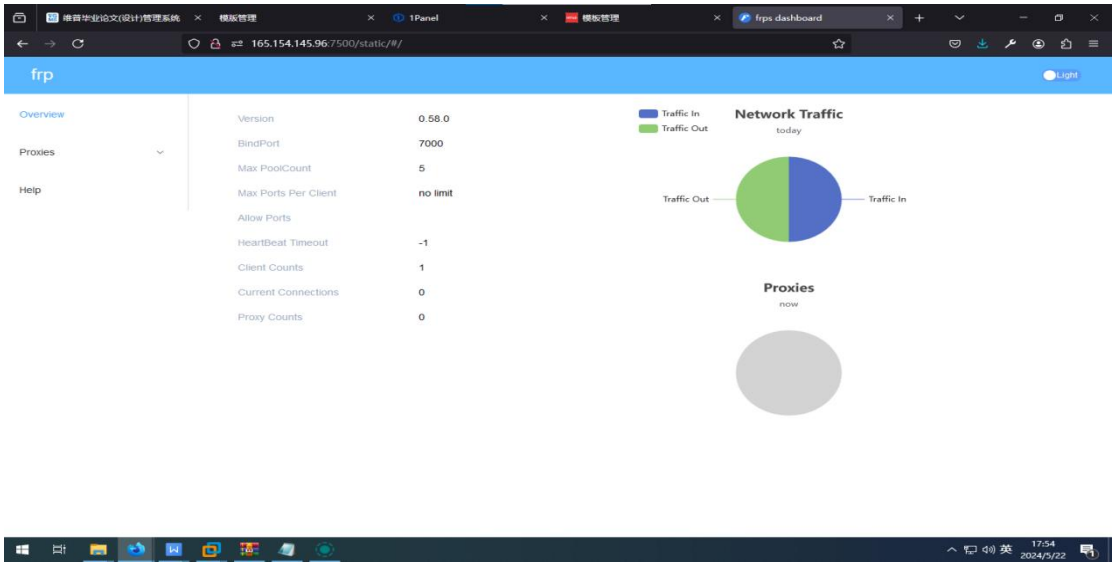


图 5-11 服务器端公网暴露 IP

为了测试蜜罐的具体效果，我们通过扫描端口访问来模拟进行攻击，通过云

扫描工具来查看蜜罐访问情况，具体情况如图 5-12 所示。

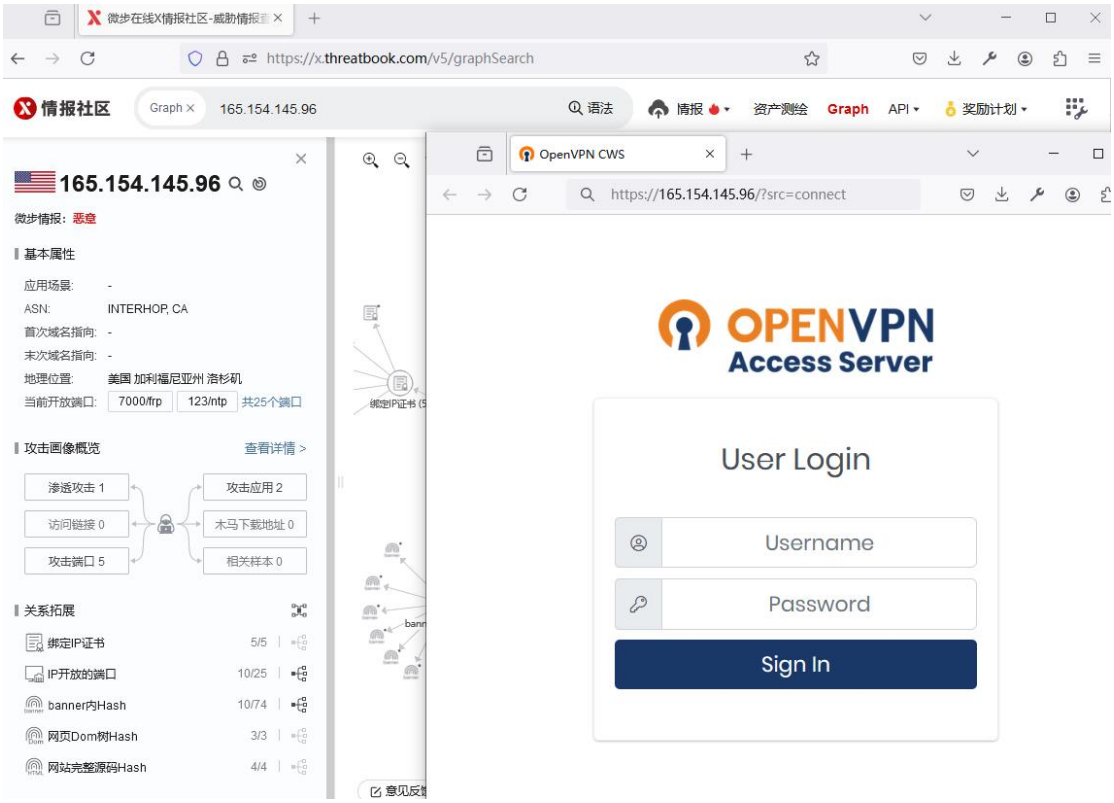


图 5-12 蜜罐伪装 OPENVPN 认证页面

5.4.2 堡垒机系统测试

主要是模拟运维人员在用户授权模式下通过 WEB 页面 SSH 链接各设备，确保各主机、网络设备、数据库、云服务等能够正常工作并及时运维。本次模拟通过将所有设备上堡垒机进行操作，其中主机终端、数据库等通过 SSH 或 RDP 进行连接、网络设备通过 Telnet 进行连接，具体资产详情如图 5-13 所示。

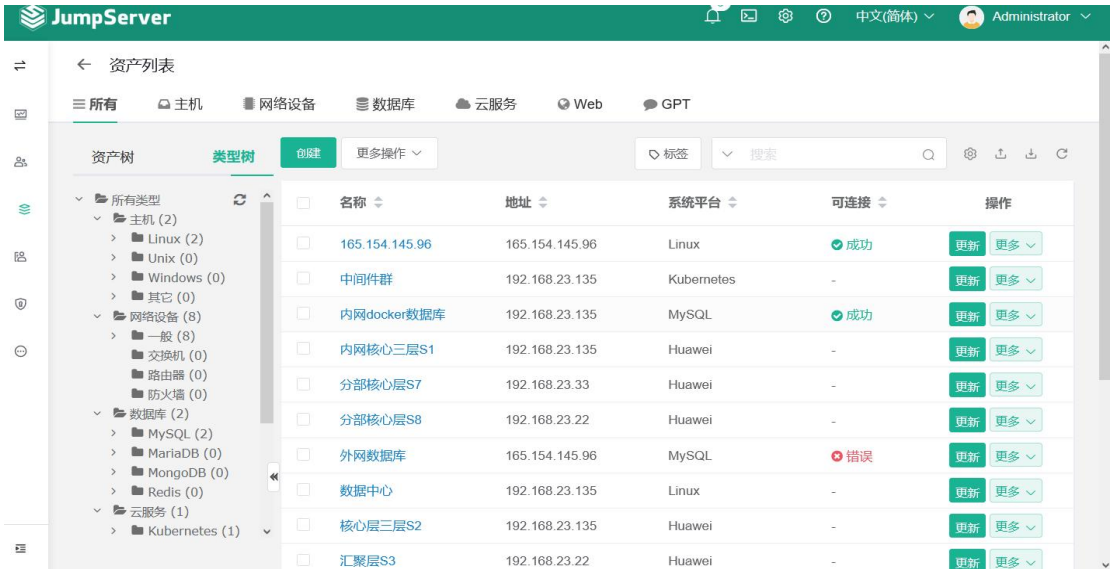


图 5-13 堡垒机资产列表

为测试堡垒机的安全可靠性，本次模拟通过 RM -RF/*（删库）命令测试堡垒机连接是否能够保证运维环境的安全。如图 5-14 所示，该危险命令被拦截，确保了服务器安全。

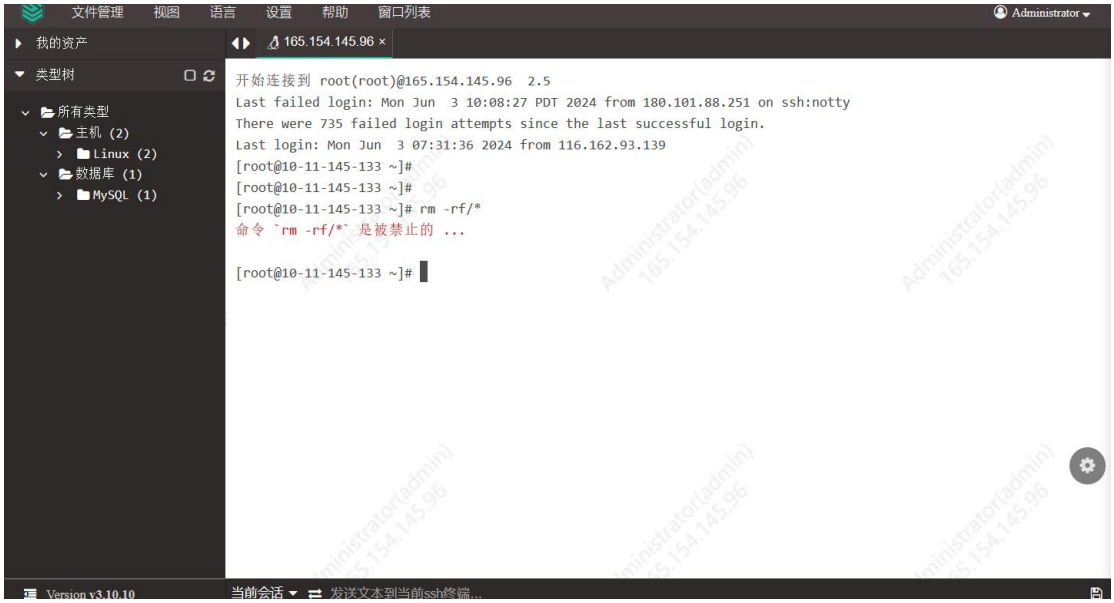


图 5-14 堡垒机中危险命令拦截

为测试堡垒机的事前认证、事中检测、事后溯源的安全需求，本次模拟通过堡垒机审计功能测试来验证安全需求是否满足。如图 5-15 所示，通过堡垒机能够做到所有命令操作的“监控”，确保运维全流程可控。

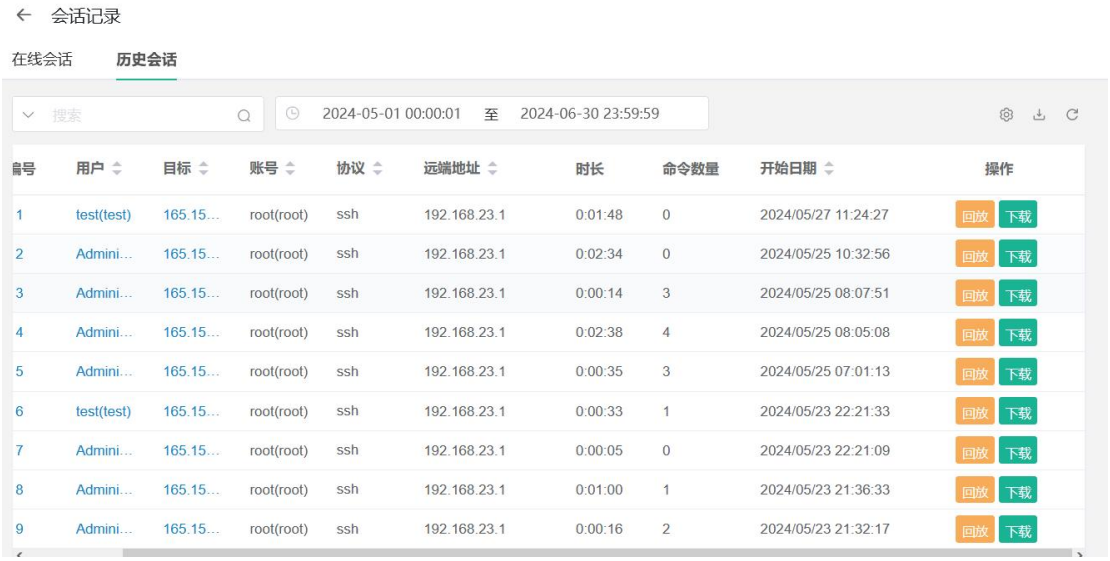


图 5-15 堡垒机会话“监控”

第 6 章 未来网络安全技术探究及总结

6.1 未来网络安全技术探究展望

第一是主动免疫可信计算，解决网络接入层一系列的安全问题。主要是通过 TPM 安全芯片实现身份认证，主要研究展望方向是基于 TPM 的可信任根实施各类安全组策略，排除恶意近源接入。

第二是数字水印技术或 DLP 系统应用到大量民用企业。

数字水印简单来讲就是通过“隐写”达到数据安全的效果。未来展望应用场景，主要以版权保护、信息隐藏、信息溯源、访问控制为主。

其中：版权保护是将版权信息嵌入、信息隐藏是“隐写”技术的一种、信息溯源是身份识别标识嵌入主要用于追踪来源、访问控制则是通过检测水印判断权限。

DLP 系统是数据安全保护的重要一环，主要通过配置该系统在核心交换机或云服务平台中来控制客户端内各类文件安全，并管控打印、读写等关键信息泄露渠道，现阶段绿盟、奇安信等网络设备厂商都提供该系统服务，但仅局限为超大企业，随着版权、保密等重要性提高，日后民间企业中，数字水印 DLP 系统等技术的重要性将更加凸显。

最后，新技术新应用安全将引发新的挑战，无论是卫星互联网的可预见未来带动了 SDR 国内部分兴趣团体的兴致；还是人工智能的大语言模型引爆人们“三观”，并且基于 Transformer、GPT 系等引发了新一轮开发热潮；新技术都带来了新挑战，卫星互联网必将使得内网隧道更加容易、人工智能必将使得网络入侵成本降到很低；但是新技术新应用带来的新挑战将是我们新时代年轻人必须面对的“新未来”。

6.2 总结

本次毕业设计通过模拟企业园区网络安全技术并进行研究，进一步论证了 ips、ids 和防火墙等被动防御和审计堡垒系统等主动防御措施能够很好的进行网络安全的防护，但是对于伪装流量、木马以及蠕虫等网络安全威胁仍旧存在些许漏洞。但是通过主机数字水印条件下的文本级别加密能够很好解决，被入侵但是数据确保安全的状况。针对于木马、伪装流量、篡改日志等入侵方法，期待后续机器学习条件下针对特征码获取、恶意流量识别、钓鱼邮件拦截等方面进行更深层次的堵漏。同时，在企业园区安全方面，从设计和实际使用过程中更突显出：“三分防、七分管”的重要性，在网络安全中培训要占大头，同时培训要根据新型入侵手法及时跟进更新培训内容。

不足之处，首先是因采用软路由做核心出口区策略，对于普通防火墙使用接口的 Untrust 和 Trust、Dmz 域模拟较少；其次是针对企业园区网络安全测试主要针对网络协议进行测试，针对云服务器的容器逃逸、WEB 服务器的注入等测试较少；还有就是在数据安全测试过程中，针对 DLP 系统（数据泄漏防护）的使用没能进行，主要是因为免费版的系统及测试环境较少，在今后如果有机会将测试 DLP 系统基于云服务和网络旁路服务的相关数据安全测试；最后就是在本次毕业设计过程中病毒的扫描器的配置是以云服务为主，IPS 模拟以软路由内置为主，大厂商的防火墙匹配库肯定相对软路由内的匹配库完善，但因版权问题和设备难模拟问题，ips 模拟没能达到预先效果。期待在今后的研究中继续完善。

参考文献

[1] 张泽洲, 王鹏. 零信任安全架构研究综述[J]. 保密科学技术, 2021, (08):8-16.

[2] 童威, 黄启萍. 基于云计算的数据安全保护关键技术分析[J]. 信息与电脑(理论版), 2021, 33(21):200-202.

[3] 金华松. 基于云计算的虚拟化环境网络数据安全防护方案研究[J]. 信息与电脑(理论版), 2023, 35(19):205-208.

[4] 刘奇旭, 靳泽, 陈灿华等. 物联网访问控制安全性综述[J]. 计算机研究与发展, 2022, 5910):2190-2211.

[5] 孙彦斌, 汪弘毅, 田志宏等. 工业控制系统安全防护技术发展研究[J]. 中国工程科学, 2023, 2506):126-136.

[6] 李向东. 基于人工智能的恶意代码检测与防范机制研究[J]. 电脑知识与技术, 2023, 19(32):69-71+77.

[7] 任华. 基于事件的网络安全威胁智能识别[J]. 江信息通信, 2021, 34(11):140-142.

[8] 陈明, 汤文峤. 智能化条件下网络威胁情报分析研究[J]. 情报杂志, 2023, 42(03):17-23+33.

[9] 蒋宁, 范纯龙, 张睿航等. 基于模型的零信任网络安全架构[J]. 小型微型计算机系统, 2023, 44(08):1819-1826.

[10]Belal Ali;Mark A. Gregory;Shuo Li;Omar Amjad Dib. Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in Multi-access Edge Computing [J].Computer Networks,2024.02.27

[11]Fatima Alwahedi;AlyaziaAldhaheri;MohamedAmine Ferrag;Ammar Battah;Norbert Tihanyi.Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models[J]. Internet of Things and Cyber-Physical Systems,2024.01.01

[12]Yanhui Liu;Jianbiao Zhang;Salman Pathan Muhammad;YijianYuan;Puzhe Zhang;Maroc Sarah;Nag Avishek. Research on identity authentication system of Internet of Things based on blockchain technology[J].Journal of King Saud University - Computer and Information Sciences,2022.11.01

致　谢

该毕业设计是我本人对大学所学理论知识的一次全面的考核，包括网络工程、WEB 服务器搭建、Linux 基本运维和 ACL 安全组策略配置等，是对我网络设备配置基本功的训练，更是对我网络设备规划设计的锻炼，能够培养我综合运用所学知识独立地分析问题和解决问题的能力，为以后工作打下良好的基础。

本次设计能够顺利完成，首先我要感谢周细义老师在本次设计中为我答疑解惑，使我有一个良好的学习环境，在设计过程中的很多技术要点，周老师都能深入浅出的给予我思路，并及时给予理论和实操上的建议；其次还要感谢学校的大力支持，让我能够自由访问知网、湖南科学院数据库等相关资料，使本次设计圆满完成；最后祝愿我的母校-湖南理工学院，明天更加美好！更祝愿！各位老师万事顺心，学术层层高；各位同学前程似锦，奔赴美好未来！