华域 WebVPN 系统 技术白皮书

摘要

该文档简要阐述了深圳华域通信技术有限公司(ShenZhen Huau Communication technology Co., Ltd.) 的荣誉产品 WebVPN 的技术特点、功能特点和技术背景，欢迎垂询。

公司名称：深圳华域通信技术有限公司
服务电话：400-6996-601
服务邮箱：service@huautech.com
公司网站：www.huautech.com
文档作者：王翔宇

版权信息

文档保证声明

注意

由于产品版本升级或其它原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

联系方式

公司地址：深圳市福田区福田街道福南社区福虹路 9 号世贸广场 A 座 1902
电　　话：400-6996-601
服务邮箱：service@huautech.com
公司网站：www.huautech.com

文档更改记录

版本	修改内容描述	修改人	日期	备注
1.0.0	文档建立	王翔宇	2020 年 4 月 30 日	
1.0.1	文档支持标准格式变更	宁新杰	2023 年 8 月 21 日	
1.0.2	内容及截图优化	王翔宇	2023 年 9 月 6 日	

术语及缩略语一览表

序号	术语及缩略语	解释说明	备注
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			

目录

公司简介

深圳华域通信技术有限公司是一家专注于域名系统、网络应用优化的高科技互联网公司。公司研发团队紧贴用户实际需求，立足“开放、创新、安全”的产品理念，立志为用户打造更加科学、高效、便捷、安全的网络优化解决方案。

产品介绍

1. 基本背景

随着互联网技术飞速发展，商业模式也打破了传统的地域局限，越来越多的企业利用互联网技术提升业务效率。利用信息化，加速业务流程；利用互联网，实现随时随地的业务响应。互联网技术已经彻底改变传统的业务办理模式，借助信息化，许多业务信息实现快速处理和共享，人员无论在何时何地，只要能连上互联网，就能实现业务的及时处理。

与此同时，业务信息网络化也带来了安全威胁：企业商业数据、用户数据等信息一旦被泄露，则会带来难以估计的损失，而一旦通讯或存储的信息被篡改，则更会带来难以估计的后果。因此业务信息化，首要关注的就是安全问题。

为解决此安全问题，最具有性价比的解决方案就是使用 VPN（Virtual Private Network 虚拟专用网）技术来构建安全的业务网络。目前常用 VPN 方式均为了解决 Lan To Lan（网对网）的安全问题，随着越来越多 Port To Lan（点对网）远程接入需求出现，此类 VPN 方式明显力不从心，且存在以下弊端：授权有限，配置复杂，终端兼容性差，弱口令风险，易被运营商屏蔽……

WebVPN 技术就应运而生，其简单易用、无需客户端、安全性强、兼容性好等特点，为其快速发展提供了有力条件。构建一个能够验证用户身份，保障其安全访问内部资源和已购外网资源，同时记录详细日志的 WebVPN 系统，已成为各企业或高校的迫切需求。

2. 产品需求

2.1. 传统 VPN 受限

在信息化发展迅猛的今天，远程办公、远程学习已成为常态，通过 VPN 方式访问资源已成为用户最常

用的方式。随着 VPN 技术的不断发展，传统 VPN 方式也暴露出众多问题：

- 授权有限，授权用户数越多，价格越高；
- 配置复杂，需要安装客户端或在浏览器里安装插件；
- 更新频繁，用户登录时必须先完成更新，否则无法使用；
- 兼容性差，对终端系统及浏览器等版本均有要求。

2.2. 业务暴漏风险

在企业信息化逐步实现常态化、规模化的同时，企业向互联网发布业务也越来越多。员工、管理者等各种角色和手机、平板电脑等多种终端均需要访问业务，易造成业务暴露信息过多，面临被恶意扫描、攻击入侵的风险。

2.3. 权限控制瓶颈

移动互联网时代到来，众多移动终端的出现，使传统 VPN 基于 IP 的静态访问控制机制逐渐落伍。此机制限制了移动终端的灵活性，无法根据用户安全状态调整访问权限，已不能有效保护核心业务资源。

2.4. 缺乏运维审计

在现今信息安全事故频发背景下，如果缺乏有效运维审计能力，一旦出现运维事故，难以进行回溯追责。自 2017 年 6 月施行的《中华人民共和国网络安全法》第二十一条（三）项规定：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。如果缺乏详细的运维日志信息，将面临严重的处罚。

3. 产品目标与特性

华域智能 WebVPN 系统以零信任安全理念为设计基础，立足企业资源访问控制需求，采用多种认证和加密技术，结合多样实际场景和多重安全防护机制，为用户提供合规账号体系、严格认证机制、完善授权模型、精准运维审计的一款 WebVPN 产品。助力用户向零信任架构迁移，帮助用户实现流量身份化、权限精细化、访问动态化、运维极简化的新一代网络安全架构。具体特性包括：

3.1. 易用性

相比于传统 VPN 系统，华域智能 WebVPN 系统无需安装专用客户端或浏览器插件，用户只需要像访问普通网站一样访问 WebVPN 页面，进行登录后即可访问内网资源，符合用户操作习惯。

3.2. 可控性

华域智能 WebVPN 系统严格控制业务资源访问权限，面向用户采用多种认证方式，严格校验用户身份，保障资源访问可控性。

3.3. 安全性

华域智能 WebVPN 系统基于零信任安全理念，采用 https 的安全 Socke 加密方式，支持常见的对称加密（DES、3DES、AES、RC5、RC6 等）和非对称加密算法（RSA、Elgamal、Rabin 等）。在使用过程中类似防火墙策略，只有配置完成的资源才能够被访问，未配置资源均无法通过 WebVPN 进行访问。

3.4. 高可用性

华域智能 WebVPN 系统为保障其业务高可用性，具有多机热备和集群负载部署方式，保证 7x24 小时不间断提供服务。

3.5. 兼容性

华域智能 WebVPN 系统跨平台性强，对操作系统没有要求，无论是 PC、智能手机、平板电脑均可使用，且对浏览器和软件版本也没有要求，IE、Firefox、Chrome、Safari 等都能使用。

4. 功能介绍

华域智能 WebVPN 系统具有 WebVPN、SSL VPN、服务器管理等多种功能，既为普通用户提供内部资源和已购外网资源的快速安全访问方式，又帮助特定用户实现特定资源访问的身份验证和权限控制。以下为华域智能 WebVPN 系统的优势功能：

4.1. WebVPN

华域智能 WebVPN 系统提供基于 Web 资源的应用访问控制，允许授权用户访问只对内网开放的 Web 业务，包括内网业务系统、已购外网资源等，实现类似 VPN（虚拟专用网）的功能。相较于传统 VPN 方式，WebVPN 具有如下优势：

- 标准 HTTP/HTTPS 协议，避免运营商封锁；
- 免客户端接入，不改变用户原有使用习惯；
- 无需浏览器插件，兼容所有标准 HTTP 浏览器；
- 终端系统无要求，兼容 IOS、Android、Windows 等终端系统。。

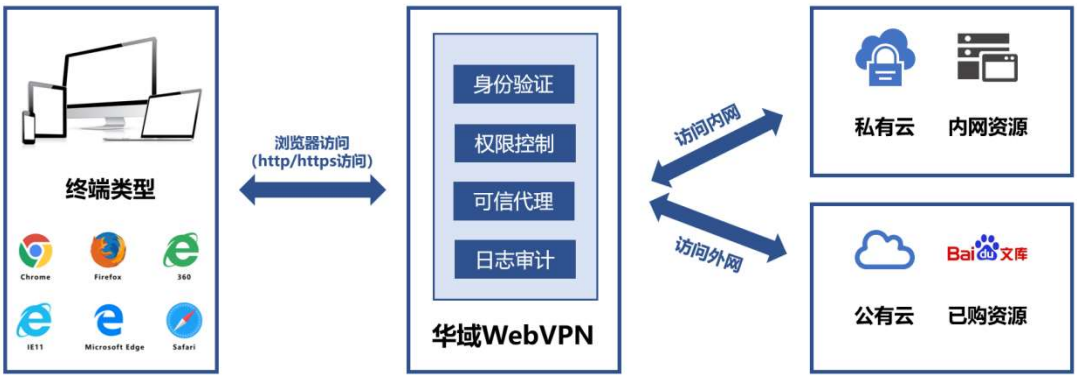

图 4.1. WebVPN 访问

4.2. 权限控制

华域智能 WebVPN 系统具有精细化控制策略，帮助用户实现多维度的访问权限控制。

- 访问终端方面：针对终端类型、浏览器类型、来源地址进行自定义管控；
- 业务资源方面：限制电子资源下载，控制资源访问流量，定义资源开放时间；
- 账户管理方面：既可以使用自带本地账户管理系统，也可以通过自助申请开通，还能够通过第三方认证系统对接实现账户快速上线；

- 用户身份方面：针对不同类型用户身份，定义不同用户权限，包括临时用户、普通用户和运维管理用户。

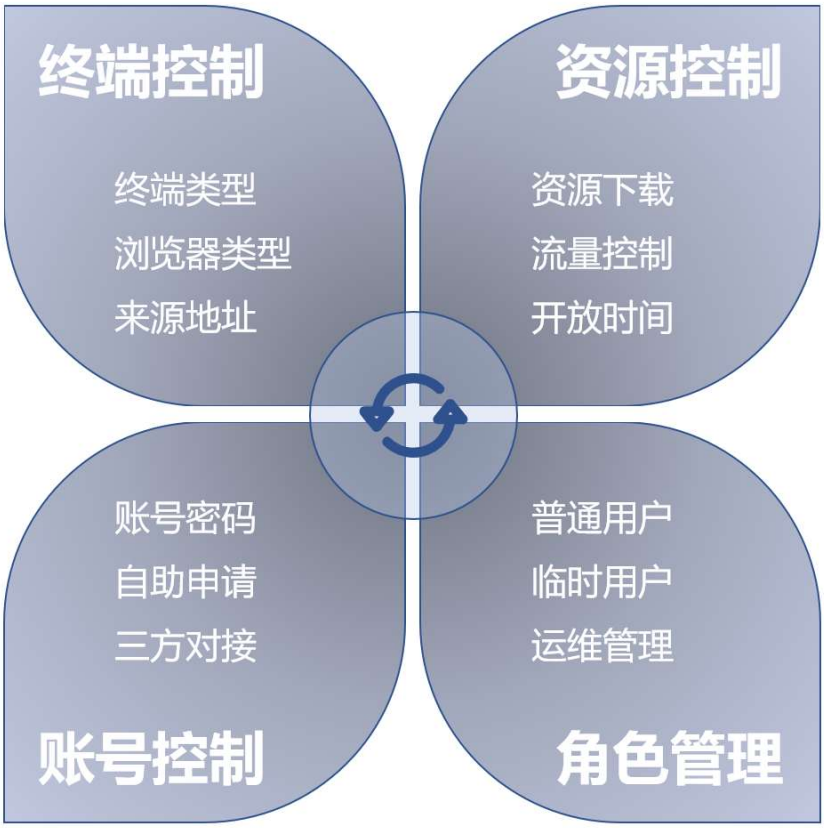

图 4.2. 权限管控

4.3. 认证防护

华域智能 WebVPN 系统集成丰富的认证方式，既支持系统自带的认证方式，包括密码、短信动态口令、验证码等，又支持与三方系统的联动认证方式，包括 CAS、LDAP、RADIUS、企业微信、钉钉等。

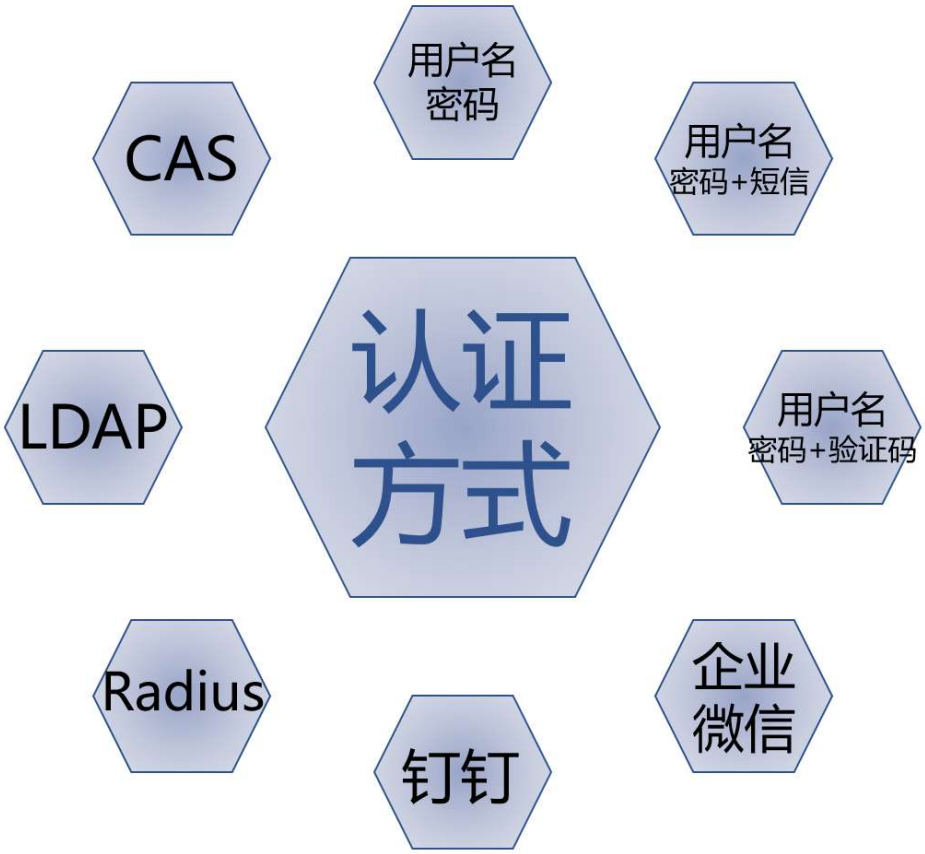

图 4.3. 认证方式

4.4. 远程协作

华域智能 WebVPN 系统集成远程协作功能，开启后原厂工程师可远程接入设备，提供原厂技术支持服务。

4.5. 远程运维

华域智能 WebVPN 系统具有服务器管理功能，以 4A（认证 Authentication、授权 Authorization、账号 Account、审计 Audit）管理理念为基础，为用户提供一套先进的运维安全管控与审计方式。通过 B/S 形式进行管理，实现对 IT 运维过程的全面监管，满足用户安全管理需求。

服务器管理功能支持 RDP、SSH、VNC、Telnet 等多种主流服务器管理协议。

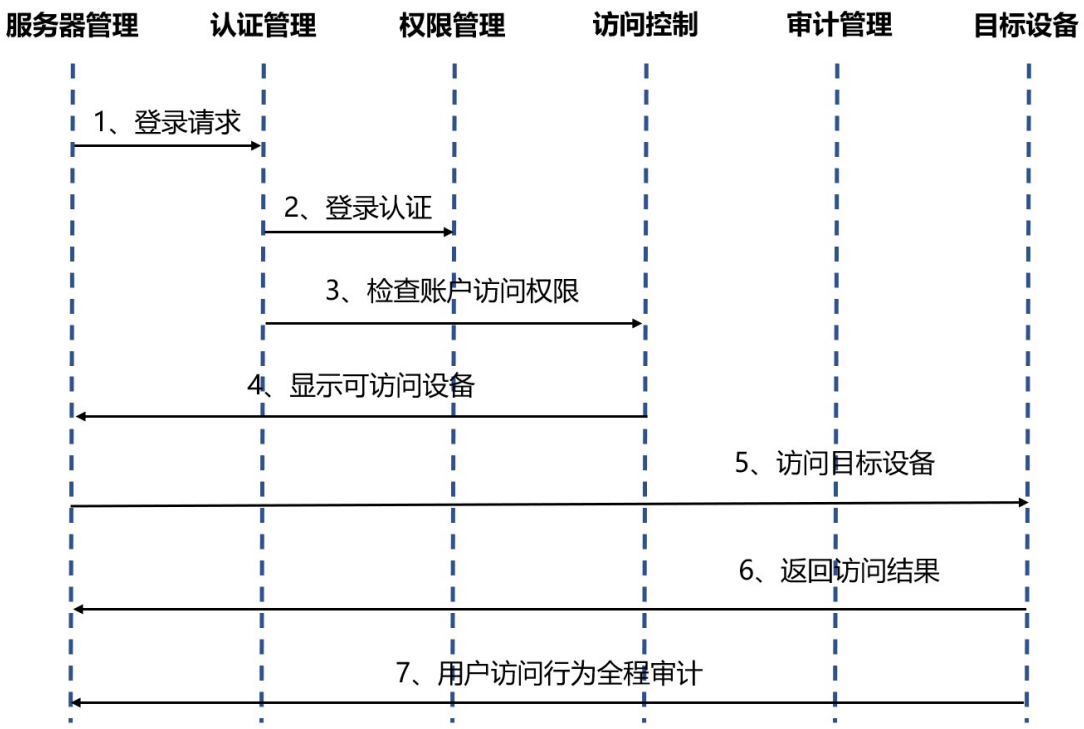

图 4.4. 远程运维

4.6. 会诊平台

在遇到需要多方协作解决的 IT 故障时，华域智能 WebVPN 系统能够为用户提供在线的远程协助会诊平台，实现以下效果：

- 一键协同：只需一键生成分享链接，协作多方即可通过该 URL 进入到同一会话界面，进行系统会诊；
- 操作权限切换：会话操作控制权可以在参与会话的用户之间进行方便的切换；
- 运维操作控制：系统管理员及会话发起者拥有会话最高权限，可全程监控会话，一旦发现会话存在危险或违规操作，可随时剥夺操作者的操作权限，甚至踢出当前会话；
- 会话过程记录：会话全过程，包括参与会诊的协同者的所有操作，均有会话录制，可供是够回溯追责，同时形成知识积累。

图 4.5. 会诊平台

4.7. 服务预警

WebVPN 系统作为用户与资源之间的重要桥梁，关键性不言而喻。为保障系统稳定性及安全性，华域智能 WebVPN 系统提供了一套完善服务预警机制，不仅可以及时发现系统异常情况，还可以帮助用户监控其它业务系统状态。

服务预警既监控自身系统运行状态，如硬件状态、服务情况等，又监控用户异常行为，如非正常频率访问，尝试破解业务系统密码等，同时支持多种即时预警方式，包括邮件、短信、语音、微信、API 等，适用于各种用户场景。

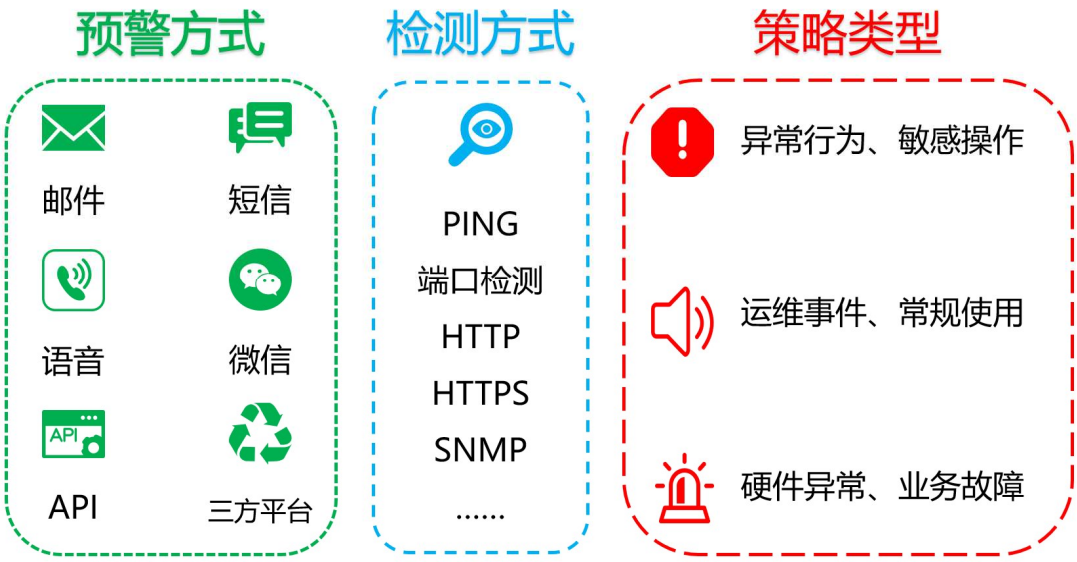

图 4.6. 预警机制

4.8. 资源访问优化

华域智能 WebVPN 系统具备完善的日志系统，并支持“日志零管理”技术。帮助用户实现：

- 日志自动维护：根据日志自动维护计划设置，系统在指定时间自动进行相应日志数据备份；
- 日志查询：系统提供多种审计日志查询条件，包括时间、账户、业务资源、关键字等；
- 分类统计：系统支持对资源访问进行分类统计，如：电子资源访问统计报表、资源下载统计报表、关键字搜索统计报表、用户下载统计报表等；
- 用户轨迹：从用户视角对海量日志进行分析提取，以时间为轴把用户所有操作串联起来，形成完整的用户资源访问体系；
- 审计报表：系统提供详细的多维度报表，既有访问量、设备类型、请求来源、资源访问变化趋势等信息的可视化报表，又有资源访问原始日志数据统计。支持 PDF、DOC 等多种格式导出，帮助管理人员全方位掌握系统运行状态、资源访问情况以及远程运维频率等信息。

4.9. 热备集群

高可用性 HA（High Availability）指的是通过尽量缩短因日常维护操作（计划）和突发的系统崩溃（非计划）所导致的停机时间，以提高系统和应用的可用性。HA 系统是目前企业防止核心业务系统因故障停机的最有效手段。

华域智能 WebVPN 系统为保障业务高可用性，支持多机热备、集群部署等高可用性部署模式，保障

WebVPN 业务稳定性，提升 WebVPN 服务可扩展性，充分利用硬件性能。同时结合系统集中管理，快速实现多台设备的策略下发。

4.10.敏感词汇过滤

华域智能 WebVPN 系统提供关键字过滤机制，过滤机制可以根据学校的政策和规定，制定敏感词汇列表，在站点访问时进行内容替换。确保与学校的需求与价值观保持一致，屏蔽违规内容。除了基本的过滤功能，还支持正则表达式，可以更全面地过滤和替换敏感内容。

5. 系统部署

华域智能 WebVPN 系统支持多种灵活部署模式，满足不同场景下用户需求。部署模式为以下几种：

5.1. 分离部署

为充分利用设备性能，华域任意独立 WebVPN 设备均可同时充当业务服务器和日志采集审计服务器角色。组内设备可仅用于 WebVPN 服务，同时通过远程日志模式将设备日志传输至业务和日志采集审计服务共存的独立设备。

5.2. 热备模式

WebVPN 设备承担着外网访问内网的桥梁作用，其稳定性、可用性十分重要。在两台设备部署情况下，通过热备技术，一旦其中一台设备故障时，业务会自动切换到另外一台备份机。在双机热备模式下，一台设备为主机，承载全部业务，另一台仅作为备机工作，只有主机故障时，才会全面接管业务。

5.3. 集群模式

站在充分利用设备性能角度，分离模式、热备模式在工作过程中均存在一定程度上的浪费。同时，为保障系统性能能够稳定、快速扩展，通常采用集群模式部署。此种部署模式下，无论多少台设备，均通过虚拟 IP 同时对外提供服务，且只要存在一个可用系统，该系统服务就不会收到影响。

5.4. 集中管理

若多台设备在实际运行过程中，均处于同一策略情况下，可采用集中管理模式，方便管理者实现快速配置，避免重复配置及人工误操作。选择其中一台为主机，其余设备为备机，通过集中管理建立连接，备机在工作工程中读取并应用主机数据库的策略配置，同时定期进行备份。当主机故障时，备机恢复至最近系统备份，防止因主机故障导致业务中断。集中管理模式可配合热备和集群模式部署。