中神通大地 EDR&DNS&URL&VPN 云控管系统介绍

1、产品介绍

中神通大地 EDR&DNS&URL&VPN 云控管系统/TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System，简称大地云控/TrustGate，是一套专业的终端网络安全防护及互联互通网络应用增值软件，可将硬件、虚拟化平台打造为 IPv4/IPv6 双栈分布式云路由器/云原生安全应用接入网关（DNS/WEB/VPC/NAT/VPN/WAF/SLB/CASG/SASE/SD-WAN），为线上线下 OS 应用软件/SaaS/PaaS 提供全面防护、互联互通的数字化安全网络底座。

硬件、虚拟化平台 + 大地云控 = IPv4/IPv6 双栈分布式云路由器
公有云、各种云 + 大地云控 = 云原生安全接入网关
（DNS/WEB/VPC/NAT/VPN/WAF/负载均衡/CASG[1]/SASE[2]/SD-WAN）
大地云控系统 + 应用/网络系统 = 安全的可运营的 AAAAA[3]内外网安全接入系统
大地云控系统 + 软件/个人资源 = 安全的 SaaS 资源变现系统

中神通大地云控集安全及效率于一身，具体功能有 EDR/XDR/EPP 安全防护全家桶（防火墙、防病毒、HIDS 入侵检测、WAF、数据库防火墙、主机安全加固、蜜罐、弱点扫描等）、IPv4&IPv6&GRE 网络接入，DNS&DDNS 域名解析代理过滤服务，WebDAV/WEB 在线代理/WEB 服务器及 WEB 代理服务器，IKEv2、WireGuard 等多种 S2S/P2S VPN 服务器，VPN/SS/TJ/SSH 路由客户端，Stunnel/TLSProxy/KMS/BT 客户端/NFS/CIFS 应用服务，NAT/路由/流量统计等功能。全部功能都配有图形界面输入、状态查询、日志留存、源 IP 控制、目的 IP 控制、时间控制、流量控制、在线帮助、视频演示等 WEB 管理界面。

“云管端”三栖，软硬件兼施，可以部署在内网、边界和云端的 X86 硬件、虚拟机平台、VPS 云服务器上，适用于绝大多数 Linux OS（服务器、桌面版、云 OS、嵌入式 OS 等）。

[1] Cloud Access Security/Storage Gateway
[2] Secure Access Service Edge
[3] 用户管理（Administration）、用户自服务门户（User Portal）、认证（Authentication）、授权（Authorization）、计费（Accounting/Billing）和日志（Audit/Log）

可用于 Linux 主机及应用的安全防护、权威智能 DNS 解析、安全 WEB 服务器、IPv4&IPv6 流畅上网、零信任 VPN 远程接入、P2P/Mesh VPN 组网、内网公网穿透、资源发布共享、SSO 用户认证、上网审计控管、流量统计控制、网络存储、加密传输、保护隐私、绿色上网等目的，是性价比高的连通及控制互联网的技术措施，能让宽带、流量、服务器的价值得到真正的体现。

以下从多个角度具体叙述中神通大地云控的各方面信息。

1.1 目的宗旨

目的：互联互通，自建自管，保护安全及隐私，From Zero to Hero

宗旨：让用户的网络带宽价值增倍

1.2 产品特点

- **“云管端”三栖，软硬件兼施**

可以部署在公有云、Windows 终端（WSL）、Linux 桌面、X86 硬件/虚拟机（私有化部署）中，适应各种网络环境。无论部署在哪里时，都有 EDR/XDR/EFF 安全防护自身安全。

- **快速灵活**

一键安装、一页开局，“批量用户设置”功能大大缩短用户设置时间；

OS 级应用，可在常见的计算平台上安装使用，为绝大多数客户端提供服务

- **全面易用**

几十种服务器、客户端网络应用，IPv4、IPv6 网络，多种加密传输协议；全功能 WEB 管理界面降低使用者的技术门槛，右键多开窗口方便并行处理；批量用户设置、策略推送等功能可降低部署成本，减少人为疏忽差错，消除软件配置的安全漏洞；

“开放服务列表”一个页面显示系统配置、全部功能及相关参数，本机状态一目了然；特制的 SHELL 批处理命令，精选多个关键命令，一键查看系统当前状态

- **安全稳定**

EDR/XDR/EFF 全方位保护主机及应用安全，包括防火墙、防病毒（文件系统实时防护）、HIDS 入侵检测、即插即用安全 WEB 服务器、WAF 防火墙、数据库防火墙、主机安全加固（自动升级系统，修补安全漏洞、安全审计、基线测试、漏洞检测、rootkit 检测、WEBSHELL 检测、弱口令检测）、蜜罐、弱点扫描、时间控制等功能；

零信任傻瓜式主机防火墙（公有云安全组可全通免配置）、用户认证、防暴力破解、免费 SSL 证书；

定期检查 CPU 及系统负载；定期检查进程健康；C 语言编译的程序（无反编译源码泄露的风险、非解释型语言运行快、可移植性好）；无 SQL 服务（内存占用小、无 SQL 注入的安全隐患）；HTTPS 加密 WEB 界面（免遭中间人窃听）；管理员及用户账号非 ssh 系统账号（最小特权、降低风险）；有所在 OS 的安全补丁提示，一键打补丁；尽量启用使用 kernel 内核模块，提高系统性能及稳定性，包括 ppp、l2tp、tun、ip_tunnel、wg、se 网桥、aes、bbr 等；

通过了绿盟、Nessus 等扫描器的安全评估；中性化服务器特征，防止被 SODAN、FOFA 等网络扫描标记，避免被零日攻击

- **自主可控可扩展**

；自建自管，无需第三方云托管，防止数据泄露，保护用户商业秘密及隐私，降低运营成本；同时拥有所有权（SSH）+使用权（WebAdmin，正常模式、只读模式）；管理员可在 SHELL 里检查、定制进程及文件，有几十个配置文件（模板）可以自定义内容；程序与 html 文件分开，可替换几十种风格的 WebAdmin 主框架；加密用户认证 API 接口方便第三方自动化操作；可以在本系统 OS 里增加第三方软件，或是安装到第三方已有应用系统中，再通过同一个 WEB 界面管理；可封装成 Docker、OS 镜像等

中神通大地 EDR&DNS&URL&VPN 云管控系统真正做到了“云管端”三栖，软硬件兼施：

●中神通大地 EDR&DNS&URL&VPN 云管控系统已经通过了阿里云、华为云、腾讯云、金山云、百度智能云、天翼云、青云、亚马逊 AWS 国际云等多家公有

云巨头的严格审核，是真正的云原生软件，既可以直接在云主机上安装使用，也可以用于多台云主机组建 VPC 网络，自建成为非官方的、高性价比的 VPC 网关，实现 NAT、VPN、WAF、负载均衡等功能，具体请见：

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1540

●中神通大地 EDR&DNS&URL&VPN 云管控系统通过了统信 UOS 应用商店及深度 Deepin 商店的适配性测试，入驻这两大应用商店，具体请见“生态适配清单”：

https://www.chinauos.com/ecology/adapt

●中神通大地 EDR&DNS&URL&VPN 云管控系统通过了银河麒麟的适配性测试，具体请见“生态适配清单”：

https://eco.kylinos.cn

1.3 应用模型

借助于云计算模型的 IaaS、PaaS、SaaS 分类，把 Linux Stack 也做同样的分类，中神通大地云控处在 PaaS 层，包括终端网络安全防护，网络服务器、客户端、路由器，以及安全的 DNS、WEB 应用服务器，具体如下图 1-1 所示。

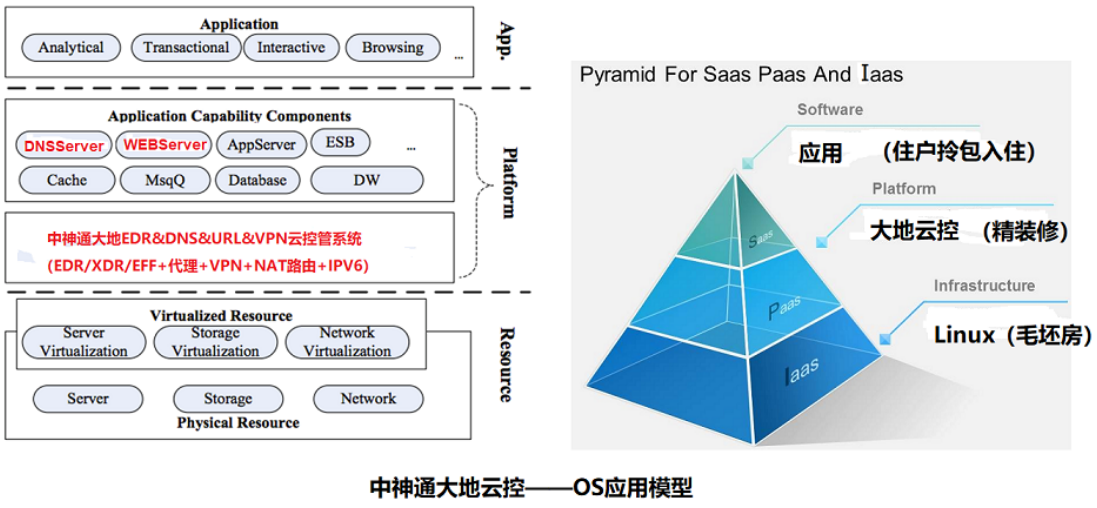
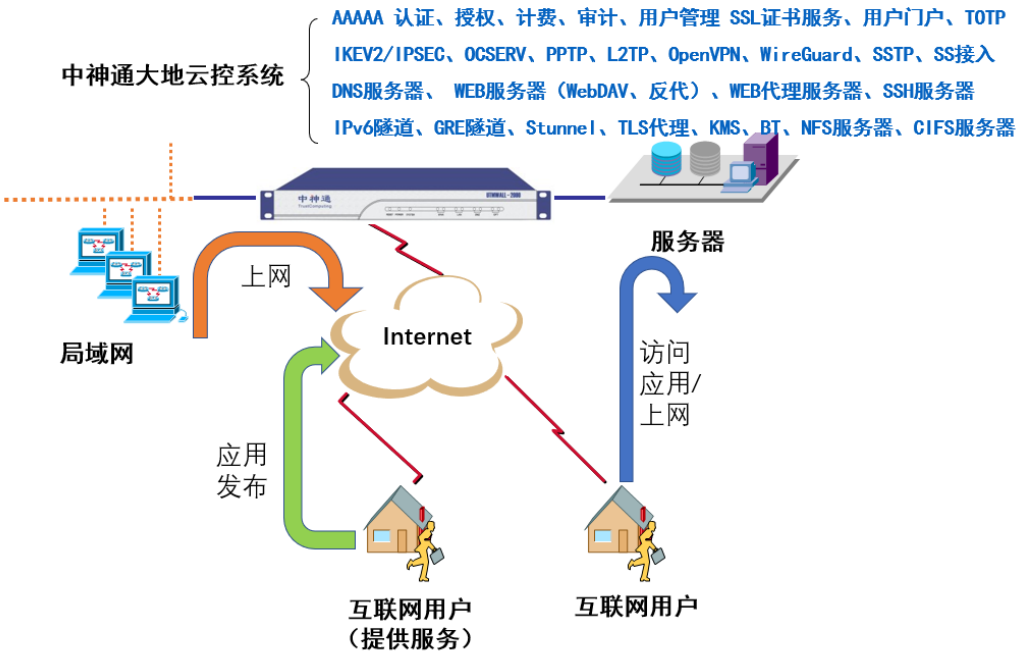


图 1-1 中神通大地云控——OS 应用模型

中神通大地云控可以部署在网络中的任意位置，大致有三种网络应用模式：用户上网、用户访问服务器、用户将自身资源映射为对外服务，具体如下图 1-2 所示。



中神通大地云控系统网络应用示意图

图 1-2 中神通大地云控——网络应用模式

1.4 产品类型

多种产品形态：硬件整机、OS 镜像（云市场镜像商品、镜像文件）、软件包。

多种产品类型：是前所未有的跨界、超融合产品，可用在 IDC/ISP/IPv6、终端及网络安全、网络存储、虚拟化云安全等多个领域，具体如下图 1-3 所示：

图 1-3 中神通大地 EDR&DNS&URL&VPN 云控管系统产品类型

就面板而言，类似于微软 Windows Server 的 Server Manager 及各个服务的控制台管理面板，如下图 1-4 所示；或者类似 Cpanel、DirectAdmin、宝塔等 WEB 主机管理面板。

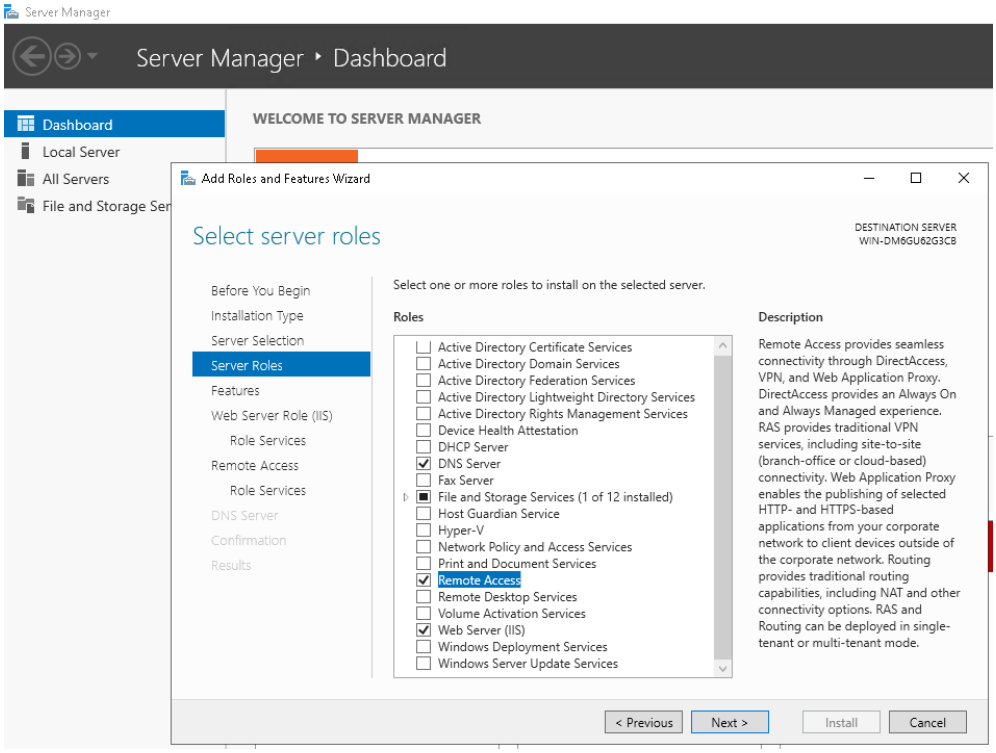


图 1-4 Windows Server 的 Server Manager

具体到 VPN 系统，中神通大地云控类似微软整套的 Always On VPN（AOVPN）4/Direct Access VPN 系统5及 Microsoft Endpoint Manager/Microsoft Intune 系统，且全部图形化管理，不需要 PowerShell 命令行工具及 XML 文件，或者类似 OpenVPN Access Server、LogMeIn Hamachi，各公有云 VPC 网关（NAT、VPN、WAF、负载均衡等）以及各种硬件、云 VPN/SDWAN/SASE/零信任网关系统的后台及 GUI 管理软件。

1.5 功能组成

中神通大地云控的功能组成具体详见图 1-5 以及表 1-1。

[4] https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy-deployment
[5] https://docs.microsoft.com/en-us/windows-server/remote/remote-access/directaccess/directaccess

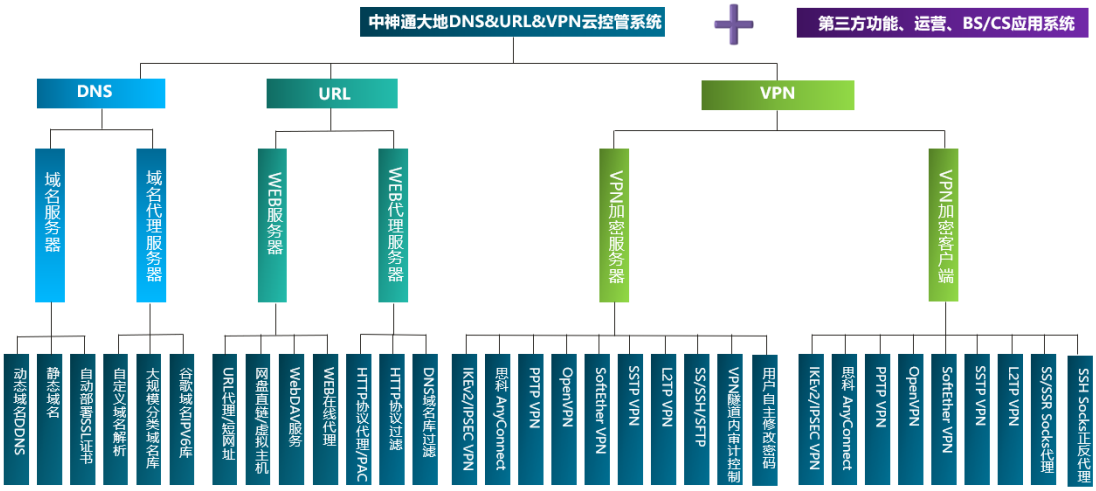


图 1-5 中神通大地 EDR&DNS&URL&VPN 云控管系统组成示意图

中神通大地 EDR&DNS&URL&VPN 云控管系统功能及优势对比表：

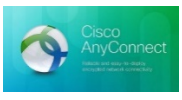
	现有软件及服务	本系统的功能	本系统的优势
1	安全狗、云锁、各大公有云 WAF 及主机安全等终端防护软件及服务	安全防护 类型：改编	全面的安全防护，包括防火墙、防病毒（文件系统实时防护）、HIDS 入侵检测、即插即用安全 WEB 服务器、WAF 代理、主机安全加固（自动升级系统，修补安全漏洞、安全审计、基线测试、rootkit 检测、WEBSHELL 检测、弱口令检测）、蜜罐、弱点扫描、时间控制等功能
2	GIP IPv6 hosts	GIP IPv6 hosts 类型：改编	自动更新域名数据 无需异地主机也可以上异地网站
3	BIND、Dnsmasq 软件	权威 DNS DNS 代理	权威 DNS，自主管理 NS 域名，A、AAAA、CNAM 等常见记录，支持泛解析；有 WEB 管

		DNS over TLS(DOT) 加密 DNS 类型：改编 智能 DNS 解析 自定义域名策略 大规模域名库 源 IP 控制、时间控制 日志留存查询 类型：原创	理面板，配置简单无差错 智能 DNS 解析功能（分区解析，不同 IP 不同结果），使用 GUI 进行配置（PowerDNS、CoreDNS 等只能手工配置，容易出错） 与系统创建的 CA 证书及 Stunnel 服务配合实现 DNS over TLS(DOT) 加密 DNS 的功能 可使用非标准端口 UDP/TCP DNS 服务器以及 DoT 服务器作为转发服务器，为本地及网络提供解析，防止 DNS 劫持 过滤 AAAA、PTR 查询，IPv4 only DNS；过滤 ANY 查询，防范 DNS 放大攻击 10 万条以上大容量自定义域名性能佳； 源 IP 控制、时间控制 日志留存及查询
4	公众 DNS 服务 CloudFlare Gateway 电信 114 、8.8.8.8 等 	DNS 代理 类型：改编 源 IP 控制、时间控制 日志留存查询 类型：原创	可使用非标准端口的 DNS 服务器，可定制服务端口，可定制域名解析内容，使之成为专属 DNS 可通过 GRE 隧道发布异地服务 可防范 DNS 放大攻击 源 IP 控制、时间控制+流量统计 源 IP 控制、时间控制 日志留存及查询
5	DDNS 服务 DynDNS、3322、花生壳	DNS 代理 自定义域名策略 类型：改编 源 IP 控制、时间控	将真实域名的 NS 记录指向本系统，即可管理该域名下的子域名 无需购买真实域名，只需将 DNS 服务器设置为本系统即可查询 多种客户端更新方式：nsupdate 客户端，

		制、流量统计 日志留存查询 类型：原创	VPN、SSH 客户端以及 URL，可更新 A 记录及 TXT 记录 URL 方式兼容 DynDNS、3322 服务器，可代替收费的服务器 自动生成 nsupdate 客户端更新批处理文件 源 IP 控制、时间控制、流量统计 日志留存及查询
6	ADBlock AdGuard 	域名库-广告 日志留存查询 类型：原创	自动更新域名数据；可替换广告内容 自定义域名解析 无需安装插件 源 IP 控制、时间控制 日志留存及查询
7	绿坝 	域名库-成人 日志留存查询 类型：原创	自动更新域名数据；无需安装软件 源 IP 控制、时间控制 日志留存及查询
8	电脑管家-病毒网站过滤 	域名库-病毒 日志留存查询 类型：原创	自动更新域名数据；无需安装软件 源 IP 控制、时间控制 日志留存及查询
9	上网行为管理 	域名库 自定义域名策略 WEB 代理策略 类型：原创	部署灵活，简洁方便 路由器 DHCP 服务中的 DNS 服务器指向本系统即可实现上网行为管理、家长控制网络 日志留存及查询 源 IP 控制、时间控制 流量统计、流量控制、计费运营
10	防火墙	内置 Iptables 策略	配置方便，对各服务的流量统计一目了

	netfilter	模板，用于访问控制和流量统计 SNAT、DNAT 策略 类型：应用 WEB 设置界面 流量统计界面 类型：原创	然，真正能解决资源被滥用的问题 防止 VPN 建立后，客户端通过 WEBRTC 等途径的 IP 泄露 IPv4、IPv6 双栈安全策略 WEB 管理界面只需填写来源 IP 即可实现防火墙保护，即源 IP 控制；另外有目的 IP 控制和时间控制 “开放服务列表”可以显示当前系统提供的所有对外服务 SNAT 来源地址转换、DNAT 目的地址转换
11	Fail2ban 防暴力破解 FAIL2BAN	内置策略模板，用于控制应用类型及发现暴力破解时的响应 类型：应用	可以对 WebAdmin、WEB 服务器、WEB 代理服务器、SSH 服务器等进行防暴力破解防护 结合 Iptables 防火墙的“源 IP 控制”及用户密码长度及复杂度的限制，可以为需要用户认证的服务提供密码安全防护
12	Squid、CCProxy、TMG 等 HTTP 代理的 URL 网址过滤	WEB 代理 类型：改编 WEB 代理策略 域名库 自定义域名策略 源 IP 控制、时间控制、流量控制 日志留存查询 类型：原创	HTTP 及 HTTPS 代理，使用本机自签名 CA 证书（双因子认证）或本机申请的真实域名 SSL 证书作为 HTTPS 代理的证书，全程加密 HTTP 代理使用 SSL CA 证书解密 HTTPS URL；为了排除对 HTTP 代理的干扰，可以配合 VPN 一起使用 内置自签名 CA 系统，CA 证书下载 URL 二维码 可通过 GRE 隧道发布异地服务 用户认证、用户自服务门户、用户管理、用户日志留存功能

			结合 DNS 域名库和自定义域名策略可以过滤分类网站 可以控制并审计传输内容，包括 IP、域名、端口、文件类型等 可以过滤 https 网站 源 IP 控制、时间控制 流量统计、流量控制、计费运营 启用用户认证，只允许合法用户使用，Fail2ban 防暴力破解 WEB 代理的用户名密码
13	Squidguard 及各种 Blacklist 黑名单 	域名库 自定义域名策略 源 IP 控制、时间控制 日志留存查询 类型：原创	容量超大，占内存少 可以通过 DNS 对客户端软件做过滤 源 IP 控制、时间控制 日志留存及查询
14	WEB 在线代理 	WEB 在线代理 类型：改编 源 IP 控制、时间控制 状态查询 类型：原创	使用浏览器，无需安装客户端软件 浏览 G 系列网站，自动加 https 前缀 某些网站 https 证书已被撤消（https://mawenjian.net/），无法使用浏览器直接查看，可以使用 WEB 在线代理间接查看 一键到达：可在 URL 中直接指定网址 可通过 GRE 隧道发布异地服务 源 IP 控制、时间控制 流量统计、流量控制、计费运营 启用用户认证、用户自服务门户，只允许合法用户使用,Fail2ban 防暴力破解 WEB

			在线代理的用户名密码 内置自签名 CA 系统，CA 证书下载 URL 二维码
15	IKEV2 VPN 	IKEV2 VPN 服务器 IKEV2 VPN 客户端 S2S IPSEC VPN 类型：改编 用户管理 状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源 IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面 内置自签名 CA 系统，CA 证书下载 URL 二维码 源 IP 控制、时间控制 流量统计、流量控制、计费运营 用户名绑定虚拟 IP 用户管理、用户状态查询功能 用户自服务门户 登录日志留存及查询
16	CISCO AnyConnect VPN 	OCSERV VPN 服务器 OCSERV VPN 客户端 类型：改编 用户管理 状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源 IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面 内置自签名 CA 系统，CA 证书下载 URL 二维码

			源 IP 控制、时间控制 流量统计、流量控制、计费运营 用户名绑定虚拟 IP 用户管理、用户状态查询管理 用户自服务门户 登录日志留存及查询
17	PPTP VPN PPTP Point-to-Point Tunneling Protocol	PPTP VPN 服务器 PPTP VPN 客户端 类型：改编 用户管理 状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源 IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面 源 IP 控制、时间控制 流量统计、流量控制、计费运营 用户名绑定虚拟 IP 用户管理、用户状态查询管理 用户自服务门户 登录日志留存及查询
18	L2TP VPN L2TP Layer Two Tunneling Protocol	L2TP VPN 服务器 L2TP VPN 客户端 类型：改编 L2TP+IKEv2 组合 用户管理 状态查询 源 IP 控制、时间控制	L2TP over IPSEC 更加安全 VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源 IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面

		日志留存查询 类型：原创	源 IP 控制、时间控制 流量统计、流量控制、计费运营 用户名绑定虚拟 IP 用户管理、用户状态查询管理 用户自服务门户 登录日志留存及查询
19	OpenVPN OPENVPN®	OpenVPN 服务器 OpenVPN 客户端 类型：改编 用户管理 状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源 IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面 获取 IPv6 IP，设置 IPv6 路由 提供可定制的中文客户端软件 内置自签名 CA 系统 源 IP 控制、时间控制 流量统计、流量控制、计费运营 TOTP 动态密码认证 用户名绑定虚拟 IP 用户管理、用户状态查询管理 用户自服务门户 登录日志留存及查询
20	WireGuard VPN CloudFlare WARP WIREGUARD FAST, MODERN, SECURE VPN TUNNEL	WireGuard VPN 服务器及客户端 类型：改编 用户管理	VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源

		状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面 源 IP 控制、时间控制 流量统计、流量控制、计费运营 用户名绑定虚拟 IP 用户管理、用户状态查询管理 用户自服务门户，自动生成公钥私钥，配置文件及二维码 登录日志留存及查询
21	SoftEther VPN SoftEther VPN	SoftEther VPN 、SSTP VPN 服务器及客户端 类型：改编 用户管理 状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	VPN 客户端登录后可用资源：使用虚拟网关 IP 内置的 DNS、WEB、WEB 代理等服务，不干扰客户端 OS 路由；VPN 客户端之间互联互通；SNAT 到外网 IP VPN 客户端登录后可提供的对外服务：源 IP 的 DDNS 域名、虚拟 IP 的端口映射以及虚拟 IP 的 URL 映射 对 Linux 客户端提供 WEB 配置页面 可重置管理员密码 内置自签名 CA 系统，CA 证书下载 URL 二维码 源 IP 控制、时间控制 流量统计 登录日志留存及查询
22	SS、TJ 服务器及 SS、SSR 客户端 shadowsocks	SS 服务器 TJ 服务器 SS 客户端 SSR 客户端 类型：改编	支持 AEAD 协议，包括 chacha20-ietf-poly1305，aes-xxx-gcm 安装时设置随机密码 对 Linux 客户端提供 WEB 配置页面 提供二维码，提供 URL，提供 Socks PAC；

		二维码、URL 生成 TJ 使用 CA 证书 状态查询 源 IP 控制、时间控制 类型：原创	UDP 代理转发 源 IP 控制、时间控制 流量统计 无需安装客户端软件，直接用 Socks 或 HTTP 代理，适用于移动环境，节省电力； 登录日志留存及查询
23	SSH 服务器及 SSH/SFTP 客户端 	SSH 服务器 SSH 客户端 SFTP 客户端 类型：改编 用户管理 状态查询 源 IP 控制、时间控制 日志留存查询 类型：原创	登录后分配源 IP 的 DDNS 域名 对 Linux 客户端提供 WEB 配置页面 源 IP 控制、时间控制 TOTP 动态密码认证 流量统计、流量控制、计费运营 无需安装客户端软件，直接用 Socks5 代理/PAC，适用于移动环境，节省电力 用户管理、用户状态查询管理 用户自服务门户 登录日志留存及查询 Fail2ban 防暴力破解 SSH 用户名密码
24	PAC 在线服务 PAC	PAC 在线服务 类型：应用	为 WEB 代理的 HTTP/HTPS 代理、SS 客户端、SSR 客户端、SSH 客户端的 Socks 代理提供 PAC 在线服务，方便客户端设置； 根据 WEB 代理、SS 客户端、SSH 客户端的配置自动生成 PAC 文件 下载需要合法的用户，Fail2ban 防暴力破解 WEB 用户名密码
25	日志审计 Elasticsearch Kibana	DNS 日志 WEB 代理日志 VPN 日志	18 种日志，统计、查询、下载，留存 N 天，配合 DNS、WEB、SSH 等服务构成真实的 Honeypot 蜜罐

		类型：原创 无 SQL 的日志查询 日志留存机制 各服务器统一日志格式 与 DDNS 更新服务、防暴力破解紧密结合	内置日志空间，无需第三方存储设备 日志留存大小、天数不受硬件限制 使用者和内容的 TOP 100 统计，饼图、柱图显示 当手机使用本系统的代理功能时，可以记录各种人为和后台的请求，由此可以发现广告、后门等异常 APP
26	WEB 管理面板 WEB 服务器   	WEBAdmin WEB 服务器 Traefik 类型：改编	首次登录修改密码 管理员日志留存及查询 WEBAdmin 后台非 PHP、无 SQL，既安全又快速 页面有丰富的 URL 链接，鼠标右键点击链接，打开新窗口，可以多窗口同时工作 中英日多语种显示 Fail2ban 防暴力破解 WebAdmin 用户名密码 用户自服务门户 内置自签名 CA 系统，CA 证书下载 URL 二维码
27	云存储、OSS 对象存储、百度网盘、阿里云盘、天翼云盘、iCloud、OneDrive、DropBox、GoogleDrive、SharePoint	WebDAV 服务 类型：改编 用户管理 源 IP 控制、时间控制 类型：原创	将 VPS 变成云存储同步网盘，是运行在 https 协议下的网络邻居，容量、带宽自定义不受限，没有内容审计，没有广告，也可以在局域网内作为 NAS 使用 Windows、Linux、MacOS、安卓、iOS 等多种 OS 下挂载远程目录到文件管理器，在本地串流播放（VLC 等）、查找、创建、编辑、删除远程文件，不需要下载、上传，

			自动同步内容 内部 URL，可读可写，访问 URL 需要用户认证；公开 URL，只读，访问 URL 不需要用户认证 文件只作为普通文件或 html 文件，屏蔽了 CGI 文件接口以保证服务器安全 可以设置用户有效期，可以手工中断连接 源 IP 控制、时间控制 流量统计、流量控制、计费运营 IPv4/IPv6 源 IP 控制、时间控制 https 链接保障安全，提供免费真实 SSL 证书申请安装，无需备案；可生成自签名 CA 证书，方便下载 可作为图床、自动备份服务器，所有文件均有外部直接链接，可以自定义 URL 的域名 启用用户认证，只允许合法用户使用，Fail2ban 防暴力破解 WebDAV 用户名密码
28	网盘+外部直接链接 轻量级虚拟主机、NAS 等 	WEB 服务器 SSH/SFTP 服务器 类型：改编 用户管理 源 IP 控制、时间控制 SFTP 日志留存查询 类型：原创	SSH 用户拥有本地限量磁盘空间，可以通过 SFTP 上传、下载文件（比传统的 FTP 方式安全），可以通过不同 OS 下的工具软件实现异地异构文件同步，可在内网使用 可以以盘符的形式安装到 Windows 及 Linux 文件系统中，方便文件操作 可以设置用户有效期，可以手工中断连接

			源 IP 控制、时间控制 流量统计、流量控制、计费运营 所有文件均有外部直接链接，可以自定义 URL 的域名 https 链接保障安全，提供免费真实 SSL 证书申请安装，无需备案；可生成自签名 CA 证书，方便下载 启用用户认证，只允许合法用户使用，Fail2ban 防暴力破解 SSH/WEB 用户名密码
29	URL 短链接短网址 	WEB 服务器 VPN、SSH 服务器 类型：改编 源 IP 控制、时间控制 VPN、SSH 日志留存查询 类型：原创	自定义 URL 的域名以及路径 HTML 跳转、302 跳转、反代、在线代理；反代、在线代理可以隐藏原始 URL 来源；固定映射、开口映射 启用或停用用户认证 与 VPN、SSH 客户端配合可以获取内部网络中的原始链接 可以是 https 的形式(相当于基于 WEB 的 SSLVPN)，提供免费真实 SSL 证书申请安装，无需备案；可生成自签名 CA 证书，方便下载 源 IP 控制、时间控制 启用用户认证，只允许合法用户使用，Fail2ban 防暴力破解 WEB 用户名密码
30	Nginx 等反向代理 云加速服务 NGINX	WEB 反向代理+第三方网站防御软件-安全狗、云盾 源 IP 控制、时间控制	用户认证、管理和日志留存功能 自主性强，可以过滤 SQL 注入攻击等非法 URL 源 IP 控制、时间控制

		类型：改编	
31	SSL 证书部署 Let's Encrypt	自定义域名策略 用户管理 类型：改编	SSL 证书部署自动化 SSL 证书状态查询、管理 SSL 证书生成后可用于 WEB 服务器虚拟主机、WebDAV 服务、HTTPS 代理服务器、IKEV2、OCSERV、SSTP、TJ、Stunnel 服务器 https 域名网站无需备案 通过 IPv6 网络申请证书，域名不需要备案
32	内网穿透 NGROK、FRP、花生壳等 ngrok	VPN 服务器、客户端 SSH 服务器、客户端 IPv6 隧道 OpenVPN 客户端 类型：改编 源 IP 控制、时间控制 VPN、SSH 日志留存查询 P2P VPN & Mesh VPN 类型：原创	绕过 VPN 服务器的 P2P VPN & Mesh VPN； 为局域网机器分配公网 IPv6 IP，方便局域网机器之间及公网用户连接 VPN 客户端虚拟 IP 的端口映射，用户可通过 WEB 用户门户自定义端口映射规则； 远程管理手机、平板等移动设备中的文件 对 Linux 客户端提供 WEB 配置页面 发布内网服务器到公网 多用户管理 源 IP 控制、时间控制 流量统计、流量控制、计费运营 多 OS 平台客户端，成熟稳定 登录日志留存及查询
33	IPv6 接入 HE	IPv6 网络接入 OpenVPN 客户端 DNS 代理服务器 测试工具	可定制 IPv6 目的网络 可同时接入多个不同的 IPv6 网络实现 SD-WAN 使用非标准端口的 DNS 服务器获得正确

		WEB、WEB 代理、VPN、SSH、SS、SSH/SFTP 服务器 VPN、SSH、SS、SSR、SSH/SFTP 客户端 源 IP 控制、时间控制 类型：改编	的 IPv6 域名解析 使用 DNS64、NAT64 服务可以从纯 IPv6 网络环境中访问 IPv4 网络 自主管理 NS 域名可以设置 AAAA 记录 自动更新 Google 等 IPv6 hosts 文件 IPv6 Iptables 主机防火墙及 Fail2ban 防暴力破解 ping6、nslookup 等多种 IPv6 在线测试工具 DNS、在线代理/WebDAV/WEB、WEB 代理、VPN、SSH、SS、TJ、SSH/SFTP 等各种 IPv6 服务器 VPN、SSH、SS、SSR、SSH/SFTP 等各种 IPv6 客户端 为局域网机器分配公网 IPv6 IP，方便局域网机器之间及公网用户连接 源 IP 控制、时间控制 一键开关 IPv6
34	GRE 隧道 	GRE 隧道 类型：改编 时间控制	DNAT 端口映射 Iptables 主机防火墙及流量统计 与 VPN 一样可以建立虚拟路由，同时，无需加密、不被 ISP 阻拦或 QoS 时间控制
35	Stunnel 	类型：改编 源 IP 控制，时间控制	使用自带的 CA 证书 与 DNS over TLS 结合 源 IP 控制，时间控制及流量统计 提供规则编辑 WEB 页面
36	TLSProxy	类型：改编	源 IP 控制，时间控制及流量统计

	SNI Proxy	源 IP 控制，时间控制	提供规则编辑 WEB 页面 配合本机 DNS 服务器，实现一体化服务
37	KMS 	类型：改编 源 IP 控制，时间控制	源 IP 控制，时间控制及流量统计 为局域网用户批量激活 Win
38	BT 客户端 	类型：改编 源 IP 控制，时间控制	源 IP 控制，时间控制及流量统计 下载后的文件可通过 WEB 服务器下载
39	NFS 	类型：改编 源 IP 控制，时间控制	源 IP 控制，时间控制及流量统计 与 VPN 虚拟网关 IP 结合，实现安全方便的网络存储
40	SAMBA/CIFS 	类型：改编 源 IP 控制，时间控制	源 IP 控制，时间控制及流量统计 内置用户，可修改密码 与 VPN 虚拟网关 IP 结合，实现安全方便的网络存储（远程超融合）
41	 任务计划（Win） 快捷指令（iOS） 定时执行	类型：原创 时间定义、时间控制	主要功能模块都有“时间控制”选项，一个时间定义包含多个不重叠的时间段，每个时间段可以是 1 周中的任意一天中的任意一个时间段

表 1-1 中神通大地 EDR&DNS&URL&VPN 云控管系统功能及优势对比表

1.6 其他特点

中神通大地 EDR&DNS&URL&VPN 云控管系统安装程序集成 N 个一键安装脚

本，无需编译，甚至无需联网（防止软件供应链攻击），安装时，节省时间，提高效率，保证质量。相比而言，一键安装脚本只能安装单一服务，没有 WEB 图形管理界面，没有配置文件备份恢复功能，还存在安装客户信息泄露的隐患。

可在有限网络资源的主机上安装使用：包括纯 IPv6 主机、IPv4 NAT 主机、Docker 主机、小内存主机、OpenVZ、WSL 等。

传统/云 VPN、WEB 服务器及内网穿透都是单向接入，大地云控的接入（Access）是客户端&服务器双向的，而且是 IPv4&IPv6 双栈的，详见表 1-2，综合运用可以起到四通八达的效果，运用之妙，存乎一心，客户端应用场景详见“4.8 VPN/SS/SSR/TJ/SSH/IPv6 客户端”，IPv6 功能详见“5 IPv6 说明”。

IPv4/IPv6	网络层	应用层
客户端	➢ VPN 客户端获取新的 IPv4/IPv6 IP 及网络（可为局域网服务） ➢ 客户端 0 配置+服务器下发 VPN 路由+每用户不同路由（SD-WAN） ➢ P2P VPN & Mesh VPN ➢ DNS 客户端（非标准端口） ➢ 公共服务的 DDNS 客户端 ➢ IPv6 隧道客户端 ➢ IPv6 Google hosts 更新 ➢ GRE 隧道	➢ 反向代理、在线代理作为 WEB 客户端 ➢ SS/TJ/SSR/SSH 作为 Socks 或端口代理客户端 ➢ 利用 netch 实现 4 层路由/每应用不同路由 ➢ Stunnel 客户端 ➢ SS/SSR 全局透明 Socks 代理 ➢ 真实域名 SSL 证书请求更新
服务器	➢ SNAT、DNAT 地址转换 ➢ VPN 服务器/GRE 隧道+端口映射+Split Tunneling ➢ GRE 隧道+端口映射 ➢ DNS/DDNS 服务器 ➢ 智能 DNS 解析（不同来源不同解析结果） ➢ 大规模 DNS 域名库 ➢ Iptables 主机防火墙 ➢ 用户认证+防暴力破解+TOTP 动态密码认证	➢ WEB 代理 ➢ Socks 代理 ➢ Stunnel 服务器 ➢ WAF（https 代理） ➢ WEB 在线代理 ➢ WebDAV 存储服务 ➢ WEB 服务器/反代 ➢ SSH/SFTP 服务器

表 1-2 中神通大地 EDR&DNS&URL&VPN 云控管系统双栈双向接入表

以 VPN 为例，说明双向接入的用处。

VPN 用户连接成功后获得的网络资源及前提条件，详见下表 1-3：

网络资源	虚拟网关的服务	虚拟内网的连接	SNAT 上外网
内容	VPN 用户以加密的形式连接虚拟网关即本系统的 DNS、WEB、WEBDAV、KMS、NFS/CIFS 服务、SSH/SFTP 服务器，HTTP、HTTPS、Socks 代理、WEB 在线代理、IPv6 网络连接；本系统的 DNS 及 HTTP、HTTPS 代理有细致的上网过滤功能	VPN 用户以加密的形式连接其它在线 VPN 用户的虚拟 IP 的网络服务	VPN 用户的虚拟 IP 网络通过本系统的外网 IP 上网，可同时分配本系统的 DNS 服务器作为客户端的 DNS 服务器，并做上网过滤。即使停用 SNAT，也可以通过本系统虚拟网关的 HTTP、HTTPS 代理服务上网，不影响客户端路由
前提	本机的各网络服务可以设置为只对 VPN 虚拟网络开放，各 VPN 服务器可以停用 SNAT 上网功能	需要对方 PC 防火墙允许，OpenVPN 用户需要启用 C2C 功能	启用 SNAT 功能，下发给客户端可上网的路由

表 1-3 VPN 客户端拨号连接后获得的资源

VPN 用户连接成功后的对外服务的内容及前提条件，详见下表 1-4：

对外服务	DDNS 解析	端口映射/内网穿透	用户 URL
内容	本系统将 VPN 用户名解析为 VPN 用户连接时的公网 IP，A 或 AAAA 记录，在此基础	将在线 VPN 用户的虚拟 IP 的端口服务映射到本系统外网 IP 的相应端口，达到内网穿透的效	将在线 VPN 用户的虚拟 IP 的 80 端口 WEB 服务映射到本系统外网域名或

	上，客户端提供对外服务	果;SSH 客户端的反向端口代理与此类似，但需要客户端设置；可以由客户端 PC 防火墙控制来源 IP	IP 的 http/https URL；WEB、SSH 用户上传的文件形成的 URL
服务器 IP	用户的公网 IP	本系统的外网 IP	本系统的外网 IP
前提	用户名必须是域名的形式，且属于自主管理 NS 域名；客户端设置对外访问的内容；客户端 PC 防火墙设置允许的来源 IP	需要先设置端口映射规则，分为管理员设置和用户设置两种权限；客户端设置对外访问的内容;客户端 PC 防火墙设置允许的来源 IP	必须先设置“用户 URL”为“映射到用户文件”并绑定 IP；客户端 PC 防火墙设置允许的来源 IP

表 1-4 VPN 客户端拨号连接后可提供的服务

如果 VPN 客户端处于局域网内，局域网 PC 可以通过其 WEB 代理服务器及策略路由的方式访问其后的 VPN 网络——而不需要 VPN 拨号，类似于网到网 VPN，只是需要另外设置路由，可以由 PC 自己设置，也可以由局域网网关设置。

2、适用对象

中神通大地 EDR&DNS&URL&VPN 云控管系统适用于个人、单位及 ISP，不仅可以安装在内网、边界的物理机、虚拟机、NAS 里，还可以安装在国内外的云主机、VPS、容器 Docker 里，可以安装在应用系统所在的 OS 中，虚拟化环境中可以随 OS 一起迁徙，同时保障访问控制安全策略不变。例如：阿里云、腾讯云、华为云、天翼云、联通沃云、金山云、浪潮云、微软 Azure、亚马逊 AWS、Google Cloud 等，不管安装在什么地方，都可以对整个互联网开放服务。用户还可以以本软件系统为基础开发具有安全远程接入管理功能的 OA/MIS/销售管理等应用系统，或者集成用户注册运营面板，实现用户自服务功能。

以下是几个典型的用户使用场景：

◆ Linux 终端安全防护的应用

症状：作为云主机 OS 主力的 Linux 系统缺少有效的终端安全防护措施，导致基于 Linux 系统开发的应用系统经常受到网络攻击，同时，精通网络安全的人才人力成本高，安全狗、云锁等免费软件已经停止更新，公有云的主机安全、WAF、云托管等商业服务又太贵，普通用户用不起。

对策：1）安装中神通大地 EDR&DNS&URL&VPN 云控管系统到应用系统的服务器(Linux/WSL)中，启用 EDR/XDR/EPP 安全防护功能，包括防火墙、防病毒（文件系统实时防护）、HIDS 入侵检测、即插即用安全 WEB 服务器、WAF 代理、主机安全加固（自动升级系统，修补安全漏洞、安全审计、基线测试、rootkit 检测、WEBSHELL 检测、弱口令检测）、时间控制等功能，无论是 DNS、WEB、VPN 服务器还是其它自建应用服务器都能得到全面有效的安全防护。

◆ 互联互通/网络安全的应用

症状：单位基于互联网的 B/S、C/S 架构的应用系统，例如邮箱[6]、OA、CRM、对外公开的 WEB 服务器的管理后台等，被黑客扫描攻击、登录数据被暴力撞库破解、缺乏独立的日志审计、没有数据加密传输导致泄密。

对策：1）安装中神通大地 EDR&DNS&URL&VPN 云控管系统到应用系统的服务器或网络中，应用系统只对 VPN 虚拟内网开放，再利用本系统 VPN 的用户认证、静态虚拟 IP 分配以及数据保密传输功能，就能实现完整的零信任安全防护功能；2）还可以利用本系统的 DNS 服务功能，指定应用系统的域名为服务器的虚拟内网 IP，方便用户使用；3）使用 IKEV2/IPSEC 等 VPN 连接已有的 S2S VPN 网络及 P2S VPN 用户，或使用内核级速度快的 WireGuard VPN 代替以前老旧慢速的 VPN 系统，还可打造去中心化的 P2P/Mesh VPN 网络；4）启用 DNS、SSH、WEB 代理服务器，查询统计恶意用户行为，将不良 IP 放入 IP 黑名单中，通过大数据挖掘+蜜罐 Honeypot 的主动防御保护主机安全。

◆ ISP/IDC 的应用

症状：单位申请的域名网站都需要花时间进行实名备案，否则无法使用；没有 IPv6 网络，影响上网及网站访问效果；发布在微信、头条、淘宝中的文章无法

[6] 武汉病毒所刚说遭网络攻击，美情报机构就"拿到数据"了？ https://www.secrss.com/articles/33273

挂在单位官网上让搜索引擎收录；网站分布在不同地域，需要智能权威 DNS 解析才能让不同地域的客户访问最近的网站。

对策：1）安装中神通大地 EDR&DNS&URL&VPN 云控管系统到服务器或云主机 VPS 中，为域名自动申请 SSL 证书，5 分钟内开通 HTTPS 网站；2）运行 VPN 客户端获得 IPv6 IP 并为之分配域名，传统 IPv4 用户通过 WEB 代理等方式接入 IPv6 网络，可上国内外 IPv6 网站等；3）将微信、头条、淘宝中的文章通过 HTML 跳转、302 重定向、反向代理、在线代理等方式，用单位域名 URL 的形式发布；4）自定义域名规则中包含来源 IP 选项，并有大规模 IP 数据库，实现不同来源 IP 解析为不同的结果。

◆ **隐私保护/隐私计算的应用**

症状：在单位、酒店、机场、餐饮等提供公共宽带或 WIFI 的场合，存在网络窃听、DNS 劫持、WEB 劫持、钓鱼 WIFI 的安全隐患，无法保证网络安全及个人信息不被泄露；商业机构提供的各种网络服务需要手机号、邮箱、密码、身份证号、真实姓名、信用卡、网银账号等才能注册，还会留存日志，存在商家主动出售或被黑泄露的风险进而危及其它网络服务账号。解锁某些网站、APP 对地域、源 IP 的限制及记录，实现 IP 自由。

对策：1）在公有云中安装中神通大地 EDR&DNS&URL&VPN 云控管系统，启用在线代理、HTTPS 代理、GRE 隧道、VPN、SS、TJ、SSH、SFTP 等数据保密传输服务，再加上用户认证服务，就能实现完整的个人隐私保护功能；2）还可以利用大地云控系统的日志审计功能，检查手机、平板、PC 后台的网络请求，防止被安装后门木马。

说明：任何通过真实域名访问的，需要用户注册、在线支付的服务都不可靠，并且最后一个出口属于自己才是最安全的服务。公众版不能跨国使用。

◆ **内网公网穿透的应用**

症状：应用系统因为 OS 不兼容、数据涉密或数据库庞大，无法迁移至云端；应用系统在内网，没有网关的管理权限，或没有专用的内网穿透客户端软件，无法做端口映射让外部访问；不愿暴露个人隐私，不想上传身份证，无法使用 DDNS 服务；分布在各地内网里的网络设备需要集中管理，手机、平板内的文件系统需要通过 WEB Share 给第三方做上传下载管理。

对策：1）在云端部署中神通大地 EDR&DNS&URL&VPN 云控管系统，启用 VPN、SSH 服务，设置 VPN 端口映射规则及 SSH 端口代理范围；创建用户，启用用户门户；2）用户登录 WEB 用户门户，修改密码，自定义端口映射规则，再 VPN 拨号连接，系统自动将客户端 VPN 虚拟 IP 的端口映射到云端公网 IP 上；也可以通过 SSH 客户端软件设置反向代理端口映射，将客户端内网 IP 端口映射到云端公网 IP 上。对于有公网 IP 的主机可以使用 GRE 隧道+端口映射服务，实现公网穿透；3）无论是否处于 NAT 局域网中，任意客户端可组成绕过 VPN 服务器的 P2P VPN 和 Mesh VPN。

◆ **上网管理的应用**

症状：家庭里的中小学生上网不可控，学生以学习的名义沉迷游戏、动漫等和学习无关的内容。电子教室、企事业单位的上网行为管理需求与此类似。

对策：1）将上网设备或路由器 DHCP 服务的 DNS 服务器设置为中神通 DNS&URL&VPN 云控管系统所在的 IP；或强制使用 WEB 代理服务器；2）上网设备尽量使用普通用户账户——防止修改 DNS 服务器设置；3）大地云控 DNS 库启用游戏、视频等分类，这样无需安装软件，即使无人看管或新设备也可以有效控制；4）监管者还可以在云端浏览查询统计上网 DNS 历史日志，发现 PC、手机中病毒广告扣费等灰色后台流量，浏览无 DNS 污染的网站，或是自定义域名以阻拦某些不在 DNS 库中的网站。

◆ **安全存储的应用**

症状：手机照片、数据文件等，缺乏长期稳定安全方便自主可控可审计的存储共享方式。

对策：1）开启 VPN+网络存储的功能，让用户挂载 VPN 虚拟网关 IP 的 NFS 及 CIFS 资源，在网络邻居中操作文件；2）开启中神通大地云控系统的 WebDAV 服务，分配不同权限的用户账户，使用真实域名 SSL 证书、安全加密的 https 方式挂载远程目录到文件管理器，在本地串流播放、搜索、建改删远程文件，无需上传下载自动同步，不同地区、不同用户的 Windows、Linux、MacOS、安卓、iOS 系统的电脑/虚拟机、手机、平板、电纸书、智能盒子无需 VPN 同时挂载同一个目录，方便共享文件及自动备份；3）自定义分享文件链接的域名、URL 及认证数据； 4）开启 SSH/SFTP 服务，为每个人分配账号和磁盘空间，使用第三方软

件挂载远程目录到文件管理器，其它和 WebDAV 服务相同；5）开启防病毒功能，实现安全无毒的共享环境。

◆ **流量统计的应用**

症状：合法的认证用户滥用网络资源导致整个系统失效；传统软件、客户端 OS 网络资源需要对外服务实现资源变现。

对策：1）开启中神通大地云控系统的用户认证、用户门户、流量统计与控制功能，每种服务的每个用户设置不同的有效期和流量配额，系统定时进行流量统计及控制，超过流量配额的用户在控制期间内不能再使用，在下一个控制期间开始时又自动恢复使用；2）将用户名密码做成卡密，在发卡平台出售； 3）用户在发卡平台购买，网上支付，平台自动发货，用户得到用户名密码和用户门户登陆地址；4）用户首次登录强制修改密码，之后可以查看、连接服务资源，VPN 用户还可以设置端口映射规则，对外开放 VPN 客户端 OS 网络资源。

更多用途详见下表 2-1。

用途	对象	局域网	国内云主机	异地云主机
过滤广告 	个人、ISP	☺	☺	☺
防范色情 	个人、单位、ISP	☺	☺	☺
行为管理 	单位	☺	☺	☺
DNS 服务器	单位、ISP	☺	☺	☺

				
DDNS 服务器 	个人、单位、ISP	☺	☺	☺
代理服务器 	个人、单位、ISP	☺	☺	☺
VPN 服务器及客户端 	个人、单位、ISP	☺	☺	☺
SS 服务器及客户端 	个人、单位、ISP	☺	☺	☺
切换隐藏 IP/突破 IP 限制/刷单 	个人、单位		☺	☺
WIFI 手机审计及防护 	个人、单位	☺	☺	☺
手机免流 	个人		☺ 需配客户端	☺ 需配客户端
反 DNS 及 HTTP 流量劫	个人、单位		☺	

持 			非 80 端口 HTTP 代理+过滤广告的 DNS 服务器	
上异地网站 Google	个人、单位	☺	☺	☺
云存储、网盘、虚拟主机、文件同步 NetDisk 企业网盘	个人、单位、ISP	☺	☺	☺
短网址链接 URL SHORTENERS	个人、单位、ISP	☺	☺	☺
SSL 证书自动化部署 Let's Encrypt	个人、单位、ISP	☺	☺	☺
内网穿透 ngrok	个人、单位	☺	☺	☺
IPv6 接入、GRE 隧道 WORLD IPv6 LAUNCH	个人、单位	☺	☺	☺
Stunnel、TLSProxy stunnel	个人、单位、ISP	☺	☺	☺
KMS	个人、单位	☺	☺	☺

KMS				
CIFS、NFS samba	个人、单位、ISP	☺	☺	☺
BT 客户端 µTorrent	个人	☺	☺	☺

表 2-1 中神通大地 EDR&DNS&URL&VPN 云控管系统用途及部署对比表

3、平台环境

中神通大地 EDR&DNS&URL&VPN 云控管系统既可以在 X86 硬件上安装，成为一台硬件安全网关，也可以在虚拟机及 VPS、云主机上安装，成为一台云原生的云接入安全网关，它还可以对 VPN 隧道里的流量做审计和控制。

Linux 发行版本包括 CentOS、RedHat、Fedora、Amazon Linux、Oracle Linux、Aliyun Linux、OpenEuler、AlmaLinux、Ubuntu、Debian、OpenAnolis、Kali、Rocky、统信 UOS/Deepin/麒麟、SUSE、Win10 Linux（WSL/WSL2）等。

与中神通大地 EDR&DNS&URL&VPN 云控管系统兼容的虚拟化平台、云服务器、VPS、Docker、NAS 及基础 OS 供应商有且不限于以下图 3-1 所示：


腾讯云

阿里云
aliyun.com

华为企业云
HUAWEI

天翼云

百度开放云
Baidu Open Cloud

QINGCLOUD青云

沃云
Wo Cloud

金山云

美团云
MEITUAN OPEN SERVICES

inspur 浪潮云

京东云

Google Cloud

amazon
web services

Microsoft
Azure

DigitalOcean

BandwagonHOST

VULTR

linode

网易蜂巢

灵雀云
alauda.cn

时速云
tenxcloud.com

DaoCloud

Arukas

HYPER.SH

CentOS

ubuntu
Linux

debian

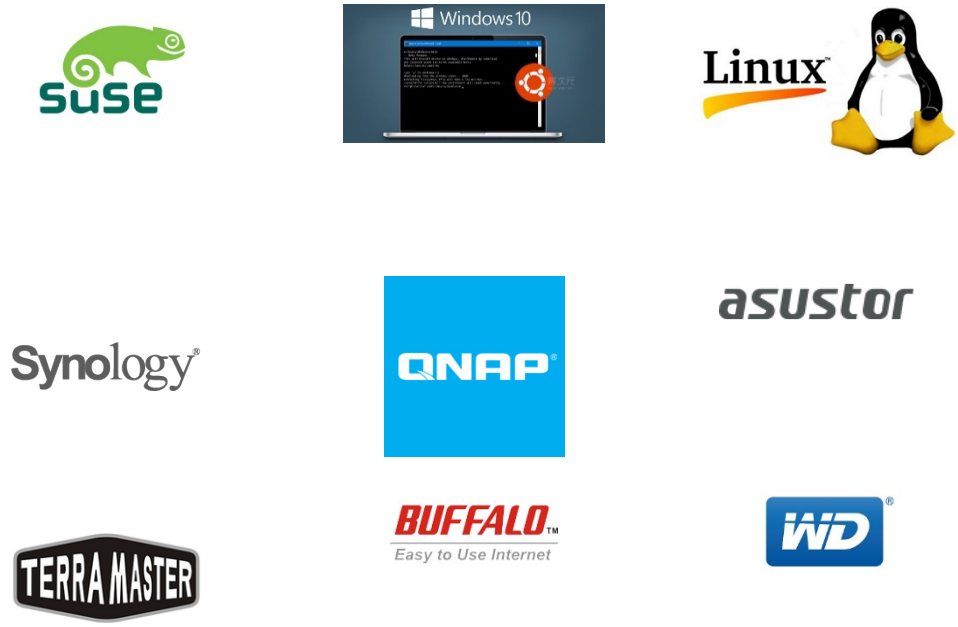


图 3-1 中神通大地云控——基础平台环境

公有云集成的 中神通 TrustComputing 大地 EDR&DNS&URL&VPN 云控管系统可代替的云存储网盘有且不限于 Dropbox、Google Drive、微软 OneDrive、天翼云盘、百度网盘、七牛云、苹果 iCloud、坚果云、腾讯微云、115 网盘、SharePoint、WEBDAV 网盘、S3 对象存储等，如下图 3-2 所示：

图 3-2 中神通大地云控——可代替网络存储平台

4、功能介绍

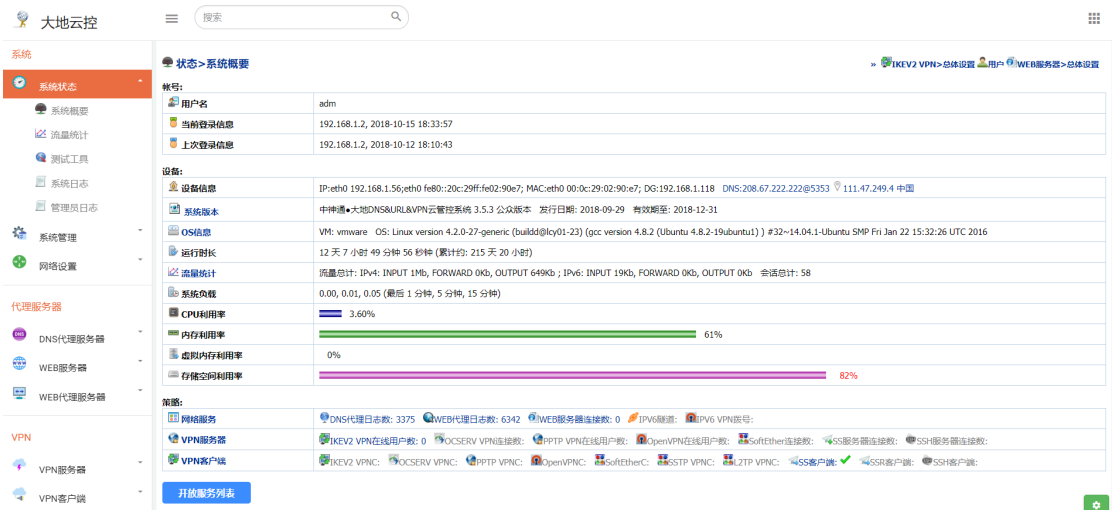


图 4-1 中神通大地 EDR&DNS&URL&VPN 云控管系统 WEB 管理界面示意图

以下功能可以在所有网卡 IP 上同时运行，系统支持 1~300 网卡 IP，IPv4&IPv6，并可以实现指定出口服务器 IP 的功能。每种功能均有配套的源 IP 控制、目的 IP 控制、时间控制与流量控制，为整个系统的安全精准运行打下了坚实的基础。

4.1 EDR/XDR/EPP 安全防护

EDR（Endpoint Detection and Response）/XDR（Extended Detection and Response）/EPP（Endpoint Protection Platform）安全防护包括防火墙、防病毒、HIDS 入侵检测、HTTPS WEB 防火墙、数据库防火墙、主机安全加固、蜜罐、弱点扫描、时间控制等功能，单机使用即可，不需要第三方注册管理（非 SaaS 模式），也无需安装 agent 客户端软件（存在软件供应链安全风险），可代替安全狗、云锁、各大公有云 WAF 及主机安全等终端防护软件及服务，保护本机（Linux 或 Windows）DNS、WEB、VPN、数据库以及其它任何自建应用服务，以下依次介绍：

1、防火墙

功能包括 Iptables 主机防火墙、SNAT 及 DNAT 端口映射、Fail2ban 防暴力破解、用户自服务门户、IPv6 总体开关以及基于规则的防 DDoS、CC 攻击等功能。

傻瓜式填表设置来源 IP 黑白名单及服务端口，可以在标准安全策略模板文件的基础上做修改，达到适配实际安全需求的目的。

生成“开放服务列表”，一个页面显示系统配置、应用服务资产清点、全部功能及相关参数。

对 WebAdmin、WEB 服务器、WEB 代理服务器、SSH 服务器等进行防暴力破解防护。

2、防病毒

功能包括本地文件实时防护以及网络防病毒服务，如果启用服务器模式，则内存至少需要 500M，服务器模式还可以为网络中其它主机提供防病毒检测服务，并定期更新防病毒数据库。

启用本地文件实时防护功能后，用户读取文件时，会先检测病毒，如果发现有病毒，则文件不可读取。如果是从 WEB 服务器上文件，则返回用户 403 错误，防止用户下载有毒文件；如果是 WebDAV、NFS、CIFS、SFTP 文件，则用户不能查看、拷贝有毒文件；如果对整盘做监控，可以防止勒索病毒、挖矿病毒、后门木马蠕虫等恶意软件的运行。

3、HIDS 入侵检测

功能包括本地文件异常检测、文件变化检测（不基于特征值，探测加密 WEBSHELL、拖库、rootkit 等异常文件，可用于网页防篡改、数据防泄露），系统日志监控，rootkit 检测，软件漏洞检测等。

4、HTTPS WEB 防火墙

是具有 WAF 功能的 HTTPS 反代服务器，可以为任意 WEB 服务器提供 WAF 防护，除了本机的 WEB 服务器，还可以为 VPN、GRE 客户端的 WEB 服务器（内网穿透）提供 HTTPS 连接、SSL 证书及 WAF 防护。和即插即用安全 WEB 服务器（**4.3**）一样，HTTPS WEB 防火墙能防护的网络攻击包括但不限于：

- SQL Injection (SQLi)：SQL 注入
- Cross Site Scripting (XSS)：跨站脚本攻击
- Local File Inclusion (LFI)：利用本地文件包含漏洞进行攻击
- Remote File Inclusione(RFI)：利用远程文件包含漏洞进行攻击
- Remote Code Execution (RCE)：利用远程命令执行漏洞进行攻击

- HTTP Protocol Violations：违反 HTTP 协议的恶意访问

5、数据库防火墙

连接真实 SQL 数据库，并过滤非法指令，保障数据库安全。

6、主机安全加固

包括 OS 升级、系统审计、基线测试等主机防护功能，通过主动实施、事前防护，确保业务连续性。

可设置自动 OS 升级，每小时检查一次官方提供的可升级软件包并自动升级（保留老版本），可以消除大部分已知安全漏洞，防患于未然。

系统审计可用于记录并追溯 SSH 远程登录等系统安全事件。

基线测试包括检查 WEBSHELL 网马、rootkit 木马、挖矿等后门程序以及弱口令、异常权限文件等不安全因素。

7、蜜罐 Honeypot

开启 DNS、SSH、WEB 服务器、WEB 代理、KMS、防暴力破解等真实服务（仿真度更高），并查看相关日志（包括/var/log 下的日志），将有恶意企图的不良 IP 加到“防火墙”的 IP 黑名单中，实现蜜罐 Honeypot 功能。可以在 WSL 中安装本系统，保护同机的 Exchange、IIS 等 Windows 服务。

8、弱点扫描

主动扫描本机或网络中其它主机，先于黑客发现 OS 及 WEB 等开放服务存在的漏洞，以利及时修补。

9、时间控制

1）功能

时间控制包括时间定义和时间控制两部分，主要功能模块都有“时间控制”选项，可实现应用的按时启用、停用的功能，一个时间定义包含多个不重叠的时间段，每个时间段可以是 1 周中的任意一天中的任意一个时间段。

2）用途

应用举例：上班时间有人值守监控，设置上班时间段为功能启用时间，可以保证有人手、有时间处理突发的安全事件。

3）适用对象

DNS WEBPROXY WEBSERVER HTTPS WAF

4）全方位控制

时间控制与源 IP 控制、目的 IP 控制、流量控制一起为整个系统的安全精准运行打下了坚实的基础

4.2 DNS 服务器

DNS 服务器包括 DNS 转发+递归查询、DNS 防火墙[7]/大规模域名库、权威 DNS 三种功能，首先，作为本地/远程 DNS 转发器，它将客户端的请求转发到 DNS 解析服务器处，并将结果缓存起来；其次，它是 DNS 防火墙/DNS Firewall，可以用来过滤客户端的请求，过滤措施包括内置的域名库和自定义域名规则；最后，它还可以作为权威智能 DNS 服务器，为整个互联网提供自主管理域名的解析服务，并提供 DDNS 客户端 IP 更新服务。

功能包括大规模 DNS 分类域名库、自定义域名规则、DNS 域名查询转发缓存、NS 自主域名管理、DDNS 服务、过滤 ANY、AAAA 等查询、SSL 证书申请安装+WEB 关联、DNS over TLS（DOT）加密 DNS 服务以及 Google IPv6 hosts 文件，以下依次介绍。

同类产品比较：

- 权威 DNS 智能解析服务：代替 DNSPod、CloudFlare、华为国际云、AWS Route53、Google Domains 等
- 自建 DNS 服务器、代理软件：Bind、CoreDNS、PowerDNS（权威 DNS 智能解析没有 GUI），Dnsmasq、 Unbound、Pi-hole（没有大规模域名库及更新服务）
- DDNS 动态解析服务：代替花生壳、3322 等
- 本地远程 DNS 递归转发缓存服务：代替路由器、8.8.8.8、114.114.114.114 等

[7] DNS 防火墙值 2000 亿美元，防御了三分之一的网络攻击
http://trustcomputing.com.cn/bbs/viewthread.php?tid=1774

- DNS 防火墙/内容过滤/行为管理：代替 ADGuard、Safebrowsing、绿坝、深信服、网康等

4.1.1 大规模 DNS 分类域名库

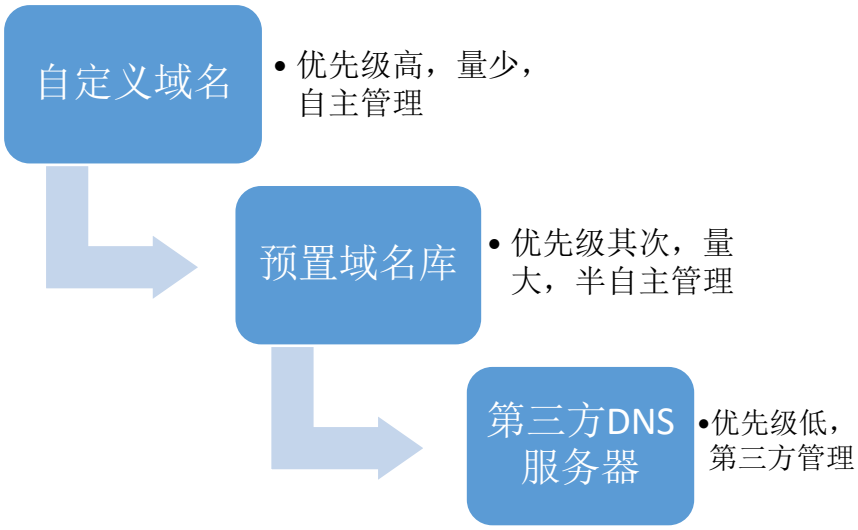


图 4-2 DNS 域名解析过程示意图

中神通大地 EDR&DNS&URL&VPN 云控管系统域名库有 23 个子类、14 万顶级域名，包括：

（1）有害无用

广告统计网站、病毒恶意网站、少儿不宜网站

（2）上传下载

代理 VPN 网站、聊天通讯网站、论坛博客网站、邮箱网盘网站、资源下载网站

（3）兼职离职

购物交易支付网站、股票彩票理财网站、兼职网赚创业网站、求职招聘猎头网站、考试留学移民网站

（4）娱乐休闲

房产家居网站、视频电影网站、音乐手机网站、文学小说网站、游戏网游网站、体育运动网站、社交交友网站、兴趣爱好网站、时尚娱乐网站、旅游汽车网站

除了 A、AAAA 记录域名解析之外，还可以通过 TXT 记录查询某个域名的具体子分类，用于第三方的日志分析、统计。

中小企业、家长即使是使用几十元的 SOHO 路由器，配合本域名库服务也可

以达到上网行为管理的目的。

4.1.2 自定义域名规则

可将某个域名的 NS 记录指向本系统，之后就可以在本系统中自主管理该域名，立即生效，无需等待，方便脚本等自动化操作，实现权威 DNS 服务器的功能。以下功能是 DNS 代理服务器功能。

（1）补充功能：可将域名库中没有的域名解析成设定的 IP

例 1：可以将“广告统计”、“少儿不宜”等子类中没有包含的网站主机名解析成本机 IP，以阻止色情广告的显示。

例 2：可以将单位内部托管的公网服务器的域名解析成其所在的内网 IP，方便单位员工从内网访问。

例 3：对启用 https 协议的网站或游戏客户端内置的服务器域名解析成本机 IP，防止员工上网看视频、游戏、购物、求职等，提高工作效率。

例 4：过滤 dnslog、C2C 服务器、黑客病毒网站的 DNS 查询，保障服务器的安全。

例 5：指纹浏览器验证代理设置时需要打开“google.com”网站，为此可以自定义 google.com 域名解析为 127.0.0.1，即本系统 WEB 服务器，这样就可以使用国内代理。

例 6：将域名的 NS 记录指向本单位的外网网关 IP，自己负责域名解析；在内网设置两套或以上的本系统，在外网（多 WAN）网关处根据源 IP 将 DNS 查询流量 53/UDP 重定向到内网不同的系统上，因此不同的客户端可以得到不同的解析结果，由此构成智能负载均衡 DNS 系统。

（2）纠正功能：将域名库中某个已有的域名解析成正确的 IP

例 1： “广告统计”子类中包含有域名 yiqifa.com，即 yiqifa.com 以及所有以 yiqifa.com 为二级域名的域名都被过滤(自定义域名也是如此)，但是很多购物辅助网站的跳转 URL 的主机名是 p.yiqifa.com，为此可以将 p.yiqifa.com 解析成正确 IP，以方便浏览。

例 2：对于 ISP、GFW 等污染了的域名同样可以在此予以纠正，将其解析成正

确的 IP，以方便浏览。

4.1.3 DNS 域名查询转发缓存功能

如果用户请求的域名不在本机自定义域名策略或预置域名库中，那么系统将向设定好的第三方域名服务器（例如：114.114.114.114 或其它提供 DNS 过滤的 DNS 服务器）转发请求，并返回解析后的 IP，查询结果会被系统缓存起来，下次再有相同的查询时会直接返回结果，从而提高了查询效率，节省了查询时间。

可使用非标准端口 UDP/TCP DNS 服务器以及 DoT 服务器作为转发服务器，同时，本 DNS 服务器也提供非标准端口 UDP/TCP DNS 服务以及 DoT 服务，为本地及网络提供解析，防止 DNS 劫持。

由于某些 ISP 会监听、污染标准 53 UDP 端口的 DNS 查询流量（IPv4、IPv6），而 Windows、Linux、安卓、iOS 等客户端都无法设置、使用非标准端口的 DNS 服务器，所以只能通过 DNS 代理服务器中转非标准端口的 DNS 服务器，才能获得正确的域名解析，或使用 DNS 代理服务器同机的 WEB 代理服务器、WEB 在线代理进行远程解析。可使用 DoT 服务器作为转发服务器，为本地及网络提供解析。

有些 VPN 客户端的 DNS 查询是通过物理网卡、非加密、标准 53 UDP 端口进行的，因此即使建立了 VPN 通道，也无法正确连接，为避免这样的 DNS 泄露，可以设置 VPN 服务器虚拟网关 IP 为 DNS 服务器。

配合 DNAT 端口映射功能可以实现 DNS 透明代理，不需要在客户端专门设置 DNS 服务器。

4.1.4 NS 自主域名管理

即自建权威 DNS 解析功能，类似各大公有云及 Cloudflare、DNSPod、geoscaling.com、3322 等提供的 DNS、DDNS 解析管理服务。

1）**域名解析**

A、AAAA、TXT、CNAME、NS、MX、NSPTR、SRV、PTR、TXT、DNAME、SPF、CAA 等常见记录，支持子域名泛解析，提供 API 方便大批量自动化操作。

另外还可以实现域名 URL 跳转功能，详见下面的“4.1.5 SSL 证书申请+WEB

关联”。

对于一个域名解析为多个 IP 的情景，提供 IP 状态监控，将失效的 IP 屏蔽，当该 IP 生效时又重新启用解析，达到自动化、高可用性、容错负载均衡的目的。

2）**智能 DNS 解析**

针对不同来源 IP，设置不同的解析类型及解析内容（分区解析），并且有大规模 IP 数据库与之配合，是 CDN、多地域 WEB 网站优化的最佳拍档，方便不同地域的用户访问最近的服务器。

应用场景 1：对外 WEB 服务器放在内网（DNAT、双线连接），外网用户、内网用户需要分别访问外网 IP 和内网 IP 才能正确的访问 WEB 服务器

应用场景 2：同一域名的 WEB 服务器分布在多个物理地点，接入不同的 ISP，需要针对不同的 ISP 用户解析为距离用户最近的 IP 地址（类似 CDN）；国外用户访问 CloudFlare CDN，国内用户访问原始网站（CloudFlare 国内访问不理想）

应用场景 3：互联网接入商 ISP 针对主流视频网站做了本地视频缓存服务，还需要针对本网络用户将主流视频网站的 IP 地址解析为本地视频缓存服务器 IP 地址

应用场景 4：对外服务只针对部分用户（部分公网或 VPN 虚拟局域网），或者需要屏蔽部分用户，他人即使知道了域名也无法访问该服务，实现私人定制功能

3）**DDNS 动态解析**

无需购买真实域名，无需实名认证，只需要将 DNS 服务器设置为本系统即可查询；如果是真实域名，事先需要将域名的 ns 记录（ns1.domain 和 ns2.domain）设置为本机公网 IP

可更新 A、AAAA 记录及 TXT 记录，10 秒刷新，立即生效，无需等待；

多种客户端更新 IP 的方式：nsupdate 客户端，VPN、SSH 客户端以及 URL；

URL 方式兼容 DynDNS、3322 服务器，可代替收费的服务器，可在 SOHO 路由器中使用；

自动生成 nsupdate 客户端更新批处理文件。

4.1.5 SSL 证书申请+WEB 关联

免费申请安装 Let's Encrypt SSL 证书，系统自动定期延续 SSL 证书有效期，并

根据用户 URL 类型的不同，设置不同的 WEB（http、https）服务的文档根目录：

- 用户 URL 类型是“302 跳转”、“反向代理”，则相当于 DNS 解析中的 URL 跳转
- 用户 URL 类型是“映射到用户文件”等，文档根目录为各个用户自己的根目录，相当于虚拟主机
  - WEB 用户通过 WebDAV 上传文件
  - SSH 用户通过 SFTP 上传文件
  - VPN 用户是其自己 OS 的 WEB 服务器文档根目录

真实域名 SSL 证书还可用于：

- VPN/WebDAV/HTTPS 代理服务，用户免下载安装自签名 CA 根证书，同时防御 MITM 攻击
- DNS over TLS（DOT）加密 DNS 服务

4.1.6 Google IPv6 hosts

（此功能已暂停）无需另外投资（异地主机、SS/VPN），配合 WEB 在线代理或 WEB 代理服务，可上异地 IPv6 网站。

注意：系统每天会自动更新数据。

4.1.7 过滤特定类型的 DNS 查询

系统拒绝对 ANY、PTR（IP 地址反查域名）类型的查询，防止 DNS 放大攻击。可以配置拒绝对 AAAA（IPv6 域名解析）的查询，实现 IPv4 only DNS，可以防止 VPN 连接时的 IPv6 地址泄露，IPv6 网络速度慢，双栈 App 打不开，提高 IPv4 网络速度。

4.1.8 DNS 日志留存

留存 A、AAAA、PTR 等正常 DNS 查询记录，以及 ANY 等非正常记录，类似 Passive DNS，可以查询、统计、压缩打包下载 DNS 日志，可用于网络审计、蜜罐、

发现网络蠕虫 botnet、态势感知、大数据挖掘等领域。

4.1.9 防 DNS 泄露

为 VPN 连接提供内置的 DNS 转发解析+大规模域名库过滤+自定义域名过滤，让 DNS 解析走 VPN 隧道，避免 VPN 客户端的 DNS 泄露。

VPN 服务器可以只下发 DNS 服务器 IP 为 VPN 路由，各 OS 都有内置的 VPN 拨号客户端，无需安装第三方 APP 软件，适用于 4G/5G 移动数据流量及 WIFI 网络环境，由此构成 DNS over VPN（DOV）解决方案，比 DNS over TLS（DOT）、DNS over HTTPS（DOH）更容易普及。

4.1.10 防 DNS 劫持

可以使用非 53 标准端口的 DNS 服务，以及 DNS over TLS（DOT）服务作为本机 DNS 解析服务器，同时，也对外提供非 53 标准端口的 UDP、TCP DNS 服务，以及 DNS over TLS（DOT）服务，防止 DNS 劫持。

配合本机的 WEB 代理、Socks 代理可以防止用户自定义 hosts 文件，逃避 DNS 过滤检查，强制按照本机的大规模域名库及自定义域名规则进行过滤。

4.3 WEB 服务器及 WEB 代理服务器

4.3.1 WEB 服务器

系统内置 apache WEB 服务器，具备 PHP、Python、CGI、SQL 等扩展接口，具备全面的 EDR（Endpoint Detection and Response）安全防护功能，使得 WEB 服务器成为即插即用的安全 WEB 服务器：

- 默认安全的文件权限设置，文档根目录、子目录、文件均为只读，防止普通用户创建、替换文件，防网页篡改、防数据泄露
- 默认没有 SQL 服务器，防止 SQL 注入；或者通过数据库防火墙连接数据库

- 中性化服务特征，防止 0day 风险牵连；安全的 SSL 等服务器配置，通过了绿盟、Nessus 等扫描器的安全评估
- 提供防火墙功能，包括黑白名单来源 IP、时间控制及防暴力破解功能，以及基于规则的防 DDoS、CC 攻击设置
- 提供内置 WAF（WEB 应用防火墙）、外置 HTTPS WAF
- 提供防病毒-文件系统实时防护
- 提供 HIDS 入侵检测+WEBSHELL 扫描
- 提供主机安全加固功能，包括 OS 自动升级（自动修复系统安全漏洞）、系统审计、基线测试、漏洞检测、WEBSHELL 检测、rootkit 检测、弱口令检测等功能
- 提供时间控制功能，保障业务可用性

WEB 服务器提供 http 和 https、IPv4 和 IPv6 、标准端口和非标准端口 WEB 服务，并内置多种 WEB 应用：

- WEB 在线代理(本地)
- WebDAV 服务（本地）
- SSH/SFTP 服务器用户上传的文件(本地)
- 源 IP 显示 API（辅助 DDNS）
- 主机信息探针
- 网络测速
- DDNS 在线更新
- SFTP WEB 客户端（本地）
- 管理员指定的 URL(HTML 跳转、302 重定向、反向代理、带 Cookie 跨网在线代理、在线代理)
- VPN 服务器登录用户的虚拟 IP(代理)
- PAC 文件（本地）
- 主页（本地）
- WEB 用户门户

URL 代理映射/短 URL 有 HTML 跳转、302 重定向、反向代理、带 Cookie 跨网在线代理、在线代理等多种形式，可启用用户认证，带用户自服务门户，可隐藏

原始 URL 来源，利用 Cookie 模拟登录，不暴露用户名密码，有固定映射或开口映射。配合 VPN/SSH/IPv6 客户端可以实现将内网、移动端等已有的 WEB 服务发布到互联网上；可以将在微博、微信、搜狐、头条、淘宝等第三方（半封闭）平台发表的文章统一用自己域名的 URL 发布，方便搜索引擎优化 SEO；配合用户认证，可实现多个资源的单点登录功能；配合自动申请 SSL 证书的域名，可以为任意网站提供 https（代理）服务。

WebDAV 服务将 VPS 变成云存储同步网盘，是运行在 https 协议下的“网络邻居”，它不受 ISP/GFW 对 139、445 端口的封锁，不受 SMB 蠕虫病毒的袭扰，加密传输不需要 VPN，有用户认证和日志，没有广告，没有内容审计，不会被和谐，容量、带宽自定义不受限，没有上传下载文件大小的限制，还可安装在内网或虚拟机中当作 NAS 使用。Windows、Linux、MacOS、安卓、iOS 等多种 OS 下挂载远程目录到文件管理器，PotPlayer、VLC、静读等多个 APP 内置 WebDAV 功能，可以查找、创建、编辑、删除远程文件，不需要下载、上传，自动同步内容，可作为游戏等程序的存盘目录，方便共享，可以在浏览器等应用中保存文件到挂载的 WebDAV 目录中，自动成为网页发布。

SSH 用户拥有本地限量磁盘空间，可以通过 SFTP 上传、下载文件（比传统的 FTP 方式安全），可以通过不同 OS 下的工具软件实现异地异构文件同步，可在内网使用；可以以盘符的形式安装到 Windows 及 Linux 文件系统中，方便文件操作。

4.3.2 WEB 代理服务器

WEB 代理服务器即安全 WEB 网关（SWG），既可以过滤内网出外网的流量，也可以作为反向代理，部署到服务器前，过滤客户端到 WEB 服务器的流量，还可以部署在远端，实现更换源 IP 的功能，用于网商刷单、游戏挂机等网赚项目。WEB 代理过滤能事前过滤客户端请求信息，100%确保没有非法数据包通过，还能过滤服务器反馈的信息，包括被压缩、分包的内容，这些都是旁路 WEB 审计过滤做不到的。还可以通过 DNAT 实现透明代理功能，浏览器客户端无需专门设置代理服务器。

WEB 代理包括 HTTP 代理和 HTTPS 代理两种：HTTPS 代理的证书既可以是本机外网 IP 自签名 CA 证书（双因子认证）也可以是由本机申请的真实域名 SSL 证书，HTTPS 代理可实现全程加密传输，作用和 VPN、SS、SSH 服务类似；HTTP 代理可以解密 HTTPS URL，为了排除对 HTTP 代理明文协议的干扰，可以使用 VPN+VIP HTTP 代理+解密 HTTPS 的解决方案。

WEB 代理服务器还有完善的细分策略，包括对 IP、域名、URL、端口、文件类型、文件大小、Agent 等做控制。可以启用用户认证功能，防止资源被滥用，即使客户端 IP 一样，也能通过用户名加以区分，并有日志记录。

为防止部分用户修改 hosts 文件躲避 DNS 代理服务器的检查，必要时可以启用 WEB 代理功能，WEB 代理服务器将优先查询本机 DNS 代理服务器的自定义域名和域名库，让域名解析强制在远程进行。同时，本 WEB 代理服务器提供 CONNECT 方法，可用于 https 网站浏览以及软件客户端的代理服务，针对异地网站，还启用了 http 强制转化为 https 的浏览方式，用户不必事先安装浏览器转换插件或设置浏览器参数就可以用任意浏览器上网浏览。

可启用用户认证，有用户管理（有效期、总流量限额），自带用户自服务门户（首次登录强制修改密码、自主修改密码、查看资源）。

提供 PAC 在线服务，方便 IE、Firefox 浏览器及移动用户使用，可以按策略使用多个 WEB 代理服务器，实现负载均衡、资源最大化的功能。

●本系统 DNS、WEB 代理和单纯的 SS/VPN 相比的优势：

1）风险低

使用本软件合法合规，而国外 SS/VPN 服务正受到执法部门从政策、技术、销售到使用的全面封堵，运营方和使用者均有风险。

2）性能好

100%不受干扰，即使放在异地也能长期稳定使用，即使是低带宽的线路表现也比 VPN 好，还可以使用第三方的网络加速软件提速。

3）花钱少：即使是安装在国内或内网甚至是 PC 虚拟机上，也能实现异地网站的上网，因而无需购买异地的云主机/VPS/SS/VPN。

4）兼容性好

智能手机、平板、电脑的安卓、IOS、Windows、MACOS、Linux 等的任意版

本，无需 root、无需越狱、无需管理员权限、无需修改文件、无需安装插件或客户端软件，任意浏览器都可以直接使用，避免有后门危害主机安全；服务端软件可在 VZ、XEN、KVM、VMWare、VirtualBox、Hyper-V、Docker、OpenStack、proxmox 等全部虚拟化平台上安装使用，可使用绝大多数 Linux OS。

5）精细管理

可以对 IP、域名、URL、端口、文件类型、文件大小等做控制，具备用户认证功能，避免非授权访问，避免使用者滥用资源，适用于企业级的科学上网。

6）日志留存

有访问日志，并且是本地留存，可以做进一步的查询和统计，避免使用者滥用资源，方便查找广告、黑客攻击等不适宜的 URL 或视频文件等隐藏的 URL 再做进一步的处理，适用于企业级的科学上网。

7）隐私性强

过滤广告、计数器等记录个人浏览习惯的网站，既可以节省包月流量费，又可以屏蔽广告的干扰，专注于内容的浏览；不存在不经过 VPN 隧道的 DNS 泄露。高级用户可独家拥有后台管理面板，避免信息及日志泄露；一个只有使用权而没有管理权和审计权的上网方法不是一个完美的方法。

8）节省电量

移动终端的客户端 APP 均不同程度的耗电，加密越强，耗电越快，本系统无需安装客户端也可以使用，在移动终端上使用续航时间长。

当异地 VPS 的 IP 因为使用 SS/VPN 而被封时，可以切换机房，即切换 IP，再安装使用本系统。另外，本系统 DNS 和 HTTP 代理服务还可以和 SS/VPN 一起使用，在其主机上安装，既可以作为 SS/VPN 的 HTTP 代理服务器（免流的做法），也可以等 SS/VPN 拨号成功后，再当作 DNS、HTTP 代理服务器使用。

4.4 VPN/SS/TJ/SSH 服务器

VPN 服务器包括 IKEv2/IPSEC VPN、CISCO AnyConnect VPN（OCSERV VPN）、PPTP VPN、L2TP VPN、OpenVPN、WireGuard VPN（最新最快）、SoftEther VPN（包含 SSTP）、SS、TJ、SSH 等服务器，大部分都配有用户管理、状态查询与管理、

SNAT、DNAT、策略推送（客户端 0 配置）功能，全部都有日志留存与查询、时间控制、源 IP 控制及流量控制功能，可以适配几乎全部 VPN/SS/TJ/SSH 客户端。

提供免费的真实域名 CA 证书申请安装续期服务，客户端不必下载安装自签名 CA 证书。VPN 客户端（包括 Windows 内置的 VPN 拨号客户端）具备开机自动连接，断线重拨功能，客户端之间可以相互访问。还可以下发本机虚拟网关 IP 的 DNS 服务器，从而在 VPN/SS/TJ/SSH 服务器用户连通后，防止 DNS 泄露，并控制其 DNS 域名解析。

IKEv2/IPSEC VPN 服务器为多用户的 P2S VPN 服务器，IKEv2/IPSEC S2S VPN 客户端为多个并发的 Site2Site VPN 端（即传统 IPSEC 网关），可以和 Cisco ASA、CheckPoint、华为、深信服、TP-Link 等硬件 VPN 设备及各大公有云虚拟 VPN 网关互联互通，能超越局域网子网重叠、（云）VPN 服务器在内网等限制，可以全面代替各类 VPN 硬件网关、公有云 VPN、NAT 网关，组成多 WAN VPC 网络。

可以是多路异质并发的 VPN 连接，可以是通讯节点连接组成去中心化 mesh VPN，也可以连通各自内网网络组成 S2S VPN 网络。

OCSERV、OpenVPN、WireGuard 等 VPN 根据用户账号下发 VPN 虚拟 IP 及 VPN 路由网络，客户端 0 配置，相当于 SD-WAN。可以无 VPN 路由、客户端 0 配置+服务器下发 VPN 路由+每用户不同路由（SD-WAN）、客户端 4 层路由/每应用不同出口路由。

IKEv2/IPSEC、OCSERV、PPTP、L2TP、OpenVPN、WireGuard、SSH 等服务器可选 2FA/MFA TOTP 动态密码认证。

WireGuard VPN 还可以组织 P2P VPN 和 Mesh VPN，联网设备直接互联，绕过 VPN 服务器，减轻 VPN 服务器的负担，不受 VPN 服务器接入带宽的限制，降低 VPN 服务器的单点故障，免受 VPN 服务器的监听审计，大幅减小延时、提高性能。

还可以下发本机虚拟网关 IP 的 DNS 服务器，从而在 VPN/SS/TJ/SSH 服务器用户连通后，防止 DNS 泄露，并控制其 DNS 域名解析。

提供“例外的路由”设置，相当于 Split Tunneling；可以将局域网或远程代理服务器设置为例外的路由，这样可以在 VPN 连通后，使用这些代理服务器上原来的网络，是基于域名的例外路由。

对于 TJ 服务，可以和 WEB 服务器共享一个对外端口，将 WEB 服务器的 HTTP 服务监听端口改成 127.0.0.1:80，TJ 服务监听原网卡的对外端口，这样用户用浏览器访问对外端口的 https 链接资源时，TJ 服务将重定向到 127.0.0.1:80 的 HTTP 服务，而用 TJ 客户端访问时将由 TJ 服务器提供服务。

类似产品：各公有云 VPC VPN 网关、LogMeIn Hamachi、OpenVPN Access Server 等 VPN 管理系统。

VPN 客户端登录后有三种可用资源：

1）使用虚拟网关 IP 内置的 DNS、WEB、WebDAV 以及 HTTP/HTTPS 代理等服务，无需 SNAT，不干扰客户端 OS 路由，还能精细化管理；

2）VPN 客户端之间互联互通；WireGuard VPN 可以组成与 VPN 服务器无关的 P2P VPN 和 Mesh VPN

3）SNAT 上外网

VPN 客户端登录后可提供三种对外服务：

1）源 IP 的 DDNS 域名

系统为 VPN/SSH 用户自动分配 DDNS 域名，用户在此基础上提供对外服务。

2）虚拟 IP 的端口映射

外网到 VPN 客户端虚拟 IP 的端口映射，实现内网穿透(详见后述)。

3）虚拟 IP 的 URL 映射

外网地址到 VPN 客户端所在机器的 WEB 服务器的 http 以及 https 的 URL 映射，方便内网用户发布 WEB 信息或传输文件。

如果 VPN 客户端处于局域网内，局域网 PC 可以通过其 WEB 代理服务器，甚至以路由的方式访问其后的 VPN 网络——而不需要 VPN 拨号，类似于网到网 VPN，只是需要另外设置路由，可以由 PC 自己设置，也可以由局域网网关设置。

系统为 SSH 用户提供至少 10M 的磁盘空间，用户可以将其作为网盘、虚拟主机空间使用，可以将其映射到 Windows 及 Linux 的一个盘符做文件操作，可以在 PC、平板、手机上使用各种同步工具进行文件同步。

系统为 VPN/SSH 用户提供 WEB 用户门户和 SSH Console 等自服务平台，用户还可以在 WEB 用户门户中修改密码，查看登录状态、可用资源及流量统计，设置外网到 VPN 客户端虚拟 IP 的端口映射规则，实现内网穿透。

中神通大地云控 VPN 服务器相比传统 VPN 硬件网关有很大的差异化优势，具体详见下表 4-1：

	传统 VPN 硬件网关	中神通大地云控 VPN 服务器	说明
VPN 协议	协议单一，主要是 IPSEC VPN、OpenVPN（SSLVPN），不支持 IPv6，缺少对 VPN 隧道流量的审计与控制；缺少真实域名 CA 证书免费申请安装续期功能，客户端部署使用不方便，存在 MITM 攻击的风险，没有 TOTP 动态密码认证，安全性不高	多种 VPN 类型，IKEV2（IPSEC 升级版）、OCSERV、PPTP、L2TP、OpenVPN/SSLVPN 、 WireGuard（最新最快）、SoftEther、SSTP 等 VPN 以及 SS、TJ、SSH，支持 IPv6 网络；具备真实域名 CA 证书免费申请安装续期功能，客户端部署使用方便，可以防 MITM 攻击；也有自签名 CA 证书功能；具有双因子及 TOTP 动态密码认证功能；具备时间控制、目的控制、流量控制功能	协议多可以连通更多的网络，适配更多的客户端；无真实域名 CA 证书时，每个客户端都要下载安装自签名 CA 证书；用户认证安全方便
部署架构	部署位置单一，部署周期长，只能部署在单位或电信机房，应用服务器需靠近 VPN 网关，还要牵电信专线，存在电源或硬件故障，无法升级硬件配置（CPU、内存、网卡），无法抵御 DDOS 等攻击；一旦 VPN 网关被黑、被非法控制，同一交换机上的应用服务器、局域网 PC 直接暴露在黑客眼前	VPN 及应用服务器均可以部署在任意位置（硬件、虚拟化平台，IDC、边界、局域网），5 分钟部署完毕，当 VPN 服务器部署在公有云上时，应用服务器可以作为 VPN 客户端部署在局域网，节省机房、专线、迁移费用，可以动态调整 VPN 服务器的 CPU、内存、网卡、带宽，依靠公有云平台抵御 DDOS 等攻击，即使 VPN 服务器被黑也无法直接入侵应用服务器、局域网，可靠性、安全性高；例外的	公有云有 VPN 网关，但不是 OS 级别，云市场也有，不过是简化版硬件虚拟机，OS 不开放，无法整合应用；都存在 VPN 协议单一，扩展性差，性价比不高的弊端

		路由+代理服务器=Split Tunneling；具备大规模用户一键开局及策略推送（客户端0配置）功能，降低部署难度；可以组成P2P VPN和Mesh VPN	
拨号VPN	对拨号VPN支持不够，分支机构需要硬件设备，VPN客户端软件收费，缺乏OS内置的VPN客户端；VPN路由设置不灵活；没有内置代理服务，VPN客户端上网不方便且不可控；没有内置DNS服务器，存在DNS泄露的风险	专业拨号VPN服务器，分支机构不需要硬件设备、公网IP，可用OS内置、免费VPN客户端；VPN虚拟网络SNAT，绑定用户名和虚拟IP；可以不改变客户端路由，可用内置的、虚拟网关IP的DNS/WEB代理（精细控制及日志审计）、WEB应用，不影响客户端本地互联网、局域网上网；局域网用户可以通过VPN客户端上VPN网络（P2S），达到网到网VPN的效果（S2S）	网到网VPN无法精确到个人，需要配对使用硬件设备，开销大；传统VPN无法审计控制VPN隧道内的流量，容易造成越权访问；改变VPN客户端路由，会造成上网混乱
VPN客户端	每个用户都要按照VPN客户端软件，每个客户端都要手工配置；拨号VPN系统只能VPN客户端访问VPN网关后的应用服务器或网络，不能反向访问；客户端之间不能相互访问；OS不能同时运行多个VPN客户端；交互式网页登录，无法自动连接，断线重拨；	VPN客户端可以通过策略推送功能获取认证信息，做到客户端0配置，降低部署成本；VPN客户端连接后，可以为局域网用户提供VPN路由，无需为每一位用户安装VPN客户端软件；VPN客户端连接后，外网到VPN客户端虚拟IP的DNAT端口映射，实现内网穿透；映射公网URL到VPN客户端虚拟IP的WEB服务器，使其成为内容提供	手机、平板等移动终端VPN拨号后，其资源可以被外界访问，不需要上传文件，不需要备案；适用于自动登录VPN的网络环境

	不适用于无盘系统	商；为 VPN 客户端公网 IP 分配 DDNS 域名；VPN 客户端互联互通；可同时运行多个 VPN 客户端，连接不同网络；VPN 客户端开机自动连接，断线重拨，适用于无交互系统，不同 PC 不同配置；可以无 VPN 路由、客户端 0 配置+服务器下发 VPN 路由+每用户不同路由（SD-WAN）、4 层路由/每应用不同路由	

表 4-1 中神通大地云控 VPN 服务器特点及优势

注意事项：

1) 有些网络环境，对 TCP 做了负载均衡，来源 IP 不固定，导致 TCP 连接总是中断，可以换成 UDP 协议的 VPN：IKEV2 VPN、OpenVPN、WireGuard VPN、L2TP VPN

2) 有些网络环境，对 UDP 做了 QoS 流控，导致网速带宽下降，可以换成 TCP 协议的 VPN：OCSERV/PPTP/Open/SoftEther/SSTP VPN，SS，TJ，SSH

3) 有些网络环境，对 GRE 等协议不做 SNAT，导致连不通，可以换成 SNAT 友好的 VPN：IKEV2/OCSERV/OpenVPN/WireGuard/SoftEther/SSTP VPN，SS，TJ，SSH

4) 有些网络环境，对 PPTP/OpenVPN、SS 等做特征过滤，导致连不通，可以换成不常见的或官方认可的 VPN：IKEV2/OCSERV/WireGuard/SoftEther/SSTP VPN

5) 有些网络环境，干扰自签名 CA 证书的 HTTPS、IKEV2/SSTP VPN、TJ 流量，可以在线申请安装真实域名的 CA 证书

6) 有些网络环境，只有 IPv6 网络，或者 IPv6 网络的流量免费，可以设置双栈 VPN/SS/SSH 服务器或使用 DNS64、NAT64 服务，方便 IPv6 用户访问 IPv4 网络资源

7) 有些网络环境，只有 IPv4 网络，可以设置双栈 VPN/SS/TJ/SSH 服务器，方便 IPv4 用户访问 IPv6 网络资源

8）VPN 隧道是双向通信的，SS/TJ/代理服务器只能客户端到服务器单向通信

9）在内网 SNAT 环境，某些 VPN 服务只能让一个设备登录，但 SS/代理服务器允

许多个用户同时使用

10）如果 OS 启用了 BBR 加速，则尽量选择 TCP 协议的服务

11）VPS/SS/TJ/SSH 服务器功能为国内网络环境服务，在其它网络环境下使用需要注意政府的法律法规

12）iOS 等手机客户端尽量使用 IKEv2 等 OS 内置的 VPN 协议，部分手机有 SOC 硬件解密加速功能，这样可以节省 CPU 资源，更省电

13)可以通过安装特定的软件实现 Windows 内置的 VPN 拨号随机启动自动拨号，无需人工交互输入，适用于无人值守或普通用户无感知的情形；Linux OS 可以通过安装大地云控系统，使用系统内置的 VPN 客户端功能（比 Windows 内置的 VPN 拨号类型更多）实现同样的目的，也可以安装在 Windows 的 WSL 中，间接实现 Windows 的 VPN 拨号功能

中神通大地云控的 VPN 客户端端口映射与传统的 DDNS、内网穿透相比，有以下的特点和优势：

1) 一次 VPN 拨号后，可同时具备 DDNS（自己的公网）和内网穿透、URL 映射（公共服务器）三种功能/服务，或只要部分功能/服务

2) 不暴露真实 IP，即使使用 CDN 也可能暴露真实 IP

3) 不需要公网 IP，即使是公网 IP，ISP 也会封端口

4) 不需要路由器、网关的管理权限，不需要网关 DNAT 端口映射

5) 不暴露其它端口，只开放需要开放的端口，用户还可以通过 WEB 用户门户或 PC 防火墙精确控制来源用户或来源 IP

6) 不受 DNS 过滤、DNS 污染的影响，没有域名解析的延迟

7) 可以使用任意固定域名做公网 IP 解析，IPv4、IPv6 均可

8) 无需暴露个人隐私，无需上传身份证才能开通服务；无需购买专门的硬件设备，纯软件实现

9) 不需要安装专门的客户端软件，防止病毒木马入侵，多平台 0 客户端直接使用 OS 自带的 VPN 拨号连接，连接就有，断开就无，和平常使用一样

10) 专用 VPN 客户端可以做到断线重拨，Windows 启动后用户登录前自动拨号，适用于无人值守

11) 内核级端口映射，非应用层代理，稳定高效；使用标准 VPN 协议，不受应用层特征过滤措施的影响

12) 清空端口映射规则或断开 VPN 连接即可中断对外服务，不影响内网用户访问

13) 可以启用/禁用客户端通过 VPN 上网，上网时通过 VPN 虚拟服务器的 HTTP/HTTPS 代理器，做精细化上网管理

14) 充分利用公有云防入侵、防 DDoS、防 CC 攻击、动态带宽、动态 CPU 内存资源的优势

15) 将多个分布的 WEB 服务器资源统一发布到一个公网 WEB 服务器域名之下，各部门自主管理自己的 WEB 服务器

16) 公网 WEB 服务器使用大地云控系统自动申请、维护的真实域名 SSL 证书

17) 客户端的 WEB 服务器可以再套 CDN，解决流量带宽性能的问题

18) 可以让用户通过 WEB 用户门户自定义端口映射+源 IP 白名单规则，实时生效，无需重拨 VPN；实时查看每端口每 IP 的流量统计

19) 可以只让管理员设置端口映射+源 IP 白名单规则，防止用户滥用资源导致端口冲突

20) 用户使用其账号密码，通过 WEB 在线更新或 VPN 拨号后，系统为其公网 IP 分配 DDNS 域名，断开 VPN 拨号后，系统撤销 DDNS 域名

21) 可以使用 IPv4、IPv6 两种网络协议，可以将 IPv6 服务发布到 IPv4 网络，反之亦然

22) 可以将 WEB 等任意服务资源映射到多个地域的公有云上，相当于主动的、用户自主可控的智能 CDN

23）支持双因子及 TOTP 动态密码认证

24）即使客户端在 NAT 局域网中，也可组成绕过 VPN 服务器的 P2P VPN 和 Mesh VPN，增强性能、可扩展性及隐私性

需要做端口映射的内部应用可以是 WEB 服务器、3389 远程桌面、本地 Socks 代理、SFTP 服务器、BT 客户端等，客户端可以是使用 Windows、安卓、iOS、MacOS、Linux 操作系统的手机、平板、PC、服务器、路由器、NAS 等网络设备、

虚拟机、云服务器等，不需要安装客户端软件。类似产品有 CloudFlare Argo Tunnel。

4.5 用户认证

中神通大地云控系统有 WEB、VPN、SSH 三种用户，用户有有效期和总流量控制，用户数量也有许可证的限制（公众版本最大 12 个，每个用户组最大 3 个用户），用户可以通过登录 WEB 用户门户（Captive Portal）或 SSH Console 的方式自主修改密码、下载软件及配置文件、二维码，另外还有一个单独的 SS、TJ 用户。具备 AAAAA 零信任特性，即用户管理（Administration）、用户自服务门户（User Portal）、认证（Authentication）、授权（Authorization）、计费（Accounting/Billing）和日志（Audit/Log），提供用户增删改 CGI 接口，用于自动化批处理和与第三方运营模板集成。

管理员有设置第三方 URL 跳转、反代、在线代理+用户认证的功能，但这样的用户不能用于 WEB、VPN、SSH 用户资源的认证，也不能登录 WEB 用户门户。

对于 WEB、WEB 代理、SSH 用户，可以启用“防暴力破解”功能，防止恶意用户猜测用户名密码。

对于 IKEv2/IPSEC、OCSERV、PPTP、L2TP、OpenVPN、WireGuard、SSH 等 7 种用户，可以启用 2FA/MFA 的“TOTP 动态密码认证”功能，防止丢失、窃听、暴力破解用户名密码。

VPN 用户可以绑定虚拟 IP，客户端 VPN 拨号连接之后，再在 VPN 隧道内，对虚拟 IP 做 DNS 等日志审计及访问控制。

日志记录中有用户登录账号、源 IP 及登录、退出的时间、访问的资源，方便日后审计。

具体用户类型及对应的网络资源详见下表 4-2：

用户类型	网络资源
WEB 用户	WebDAV 存储（网络邻居）及上传文件形成的 URL 直链（可绑定自己的域名并安装维护 SSL 证书，免备案建站，还可上 CDN）、DDNS 域名及 IP 更新服务、WEB 在线代理、WEB 代理服务器、大规模 DNS 域名库（过滤成人、广告等）、Google IPv6

	hosts
VPN 用户	VPN 拨号后的资源（虚拟网络 SNAT 访问外网、VPN 客户端的端口服务映射到公网、VPN 客户端的 WEB 资源映射为公网 URL、虚拟服务器自身的服务、VPN 客户端之间的互联）以及与 WEB 用户类似的资源
SSH 用户	Socks 代理服务器、正向端口代理、反向端口代理（内网穿透，将客户端的 WEB、WEB 代理等服务映射成公网服务）、SFTP 存储及上传文件形成的 URL 直链（可绑定自己的域名并安装维护 SSL 证书，免备案建站，还可上 CDN ） 、 DDNS 域名及 IP 更新服务
SS、TJ 用户（单个）	SS、TJ 服务器（本地 Socks 代理，可访问外网及服务器自身的服务） 、大规模 DNS 域名库（过滤成人、广告等）、Google IPv6 hosts
无需认证的用户	大规模 DNS 域名库（过滤成人、广告等）、管理员生成的 URL（HTML 跳转、302 跳转、反向代理、在线代理）、源 IP 显示

表 4-2 用户类型

用户登录账号与 DNS 自定义域名规则名称相同时，如果是域名的形式，将用于设置 NS 自主管理域名及 DDNS 域名解析，如果不是域名的形式，将用于申请真实域名 SSL 证书,并根据用户组的不同映射为不同的 WEB 服务器文档根目录。

大规模 DNS 域名库和 Google IPv6 hosts 不需要用户认证，只是 WEB 在线代理、WEB 代理服务器域名查询时的一部分。

用户认证功能与 FreeIPA 项目部分类似。

4.6 SSL 证书服务、外网 IP 定位、NAT 地址转换、日志审计

1、SSL 证书服务

1）种类

自签名 CA 证书及基于 Let’s Encrypt 的真实域名 SSL 证书

2）用途

DNS over TLS（DOT）服务器、HTTPS WEB 服务器、WebDAV、HTTPS 代理服务器、HTTP 代理服务器-解密 HTTPS、IKEV2、OCSERV、SSTP VPN、TJ、Stunnel 服务器

3）自签名 CA 证书

服务器地址是 IP 或虚拟的域名（配合 hosts 文件或专用 DNS 服务器使用），用户事先通过 WEB 用户门户或管理员分发获得并 CA 证书，加上用户认证，相当于双因子认证，适用于单位 Intranet 应用

4）真实域名 SSL 证书

服务器地址是真实的域名，管理员一键申请真实域名证书，系统自动续期证书有效期；用户直接用域名登录，不需要安装 CA 证书，适用于 Internet 应用

类似这样的第三方免费服务的客户端还有 Duck DDNS 客户端、TunnelBroker IPv6 客户端、Speedtest.net 测速客户端等。

2、外网 IP 定位

1）分类

公网 IP、OS 外网 IP、外网地址字符串、SSL 证书中的外网地址以及 IPv6 IP

2）用途

用于设置 DNS 服务器 IP；确定客户端配置文件、PAC 文件、共享 URL 中的服务器地址；确定各服务的服务器地址

3）初始化

第一次启动 OS 时，获得公网 IP 信息，并设置外网地址字符串、及 SSL 证书中的外网地址为公网 IP，修改 HTTPS WEB 服务器、WebDAV、HTTPS 代理服务器、IKEV2、OCSERV、SSTP VPN、TJ 服务器的 SSL 证书配置并重启服务；设置 OpenVPN 服务器的例外路由；根据国内外地域不同，设置 DNS 服务器 IP

4）资源列表

根据外网 IP 地址的不同用途及本机当前运行的服务，生成“开放服务列表”文件，全面总结当前对外的服务资源；可以在用户门户中查看适用于当前用户的服务资源

3、NAT 地址转换

1）功能

NAT 地址转换包括 SNAT 源地址转换和 DNAT 目的地址转换两种类型，SNAT 用于内网、VPN 虚拟网络出外网时，将其来源 IP 地址转换为本机外网 IP 地址，DNAT 用于外部网络访问本机 OS IP 地址时，将目的地址转换为内网 IP（负载均衡）、VPN 虚拟网络 IP（内网穿透）或者 127.0.0.1（用于 DNS、WEB、SS 等全局透明代理）。

2）用途

在公有云等环境中，可以在普通云主机的基础上自建 VPC 网关，实现 NAT、VPN、DNS 等功能，只需要一个公网 IP，其它云主机都是内网 IP，由此构建多 WAN VPC 网络，可以降低成本（公有云官方的 NAT、VPN、DNS、VPC 网关一般比优惠价的云主机定价高）、扩展功能（公有云官方的 NAT、VPN、DNS、VPC 网关一般比大地云控功能少）、统一管理（集 N 种功能于一身，兼容多云、虚拟及硬件平台）。

在大中型 S2S VPN 网络中，为了避免 VPN 子网网段冲突，需要把 VPN、NAT 功能放在一台设备中，而公有云官方 VPN、NAT 网关通常是两台设备，无法满足这类需求，只能用大地云控自建一体化 VPN、NAT、DNS、VPC 网关，打造第二个 WAN 出口。

3）相关功能

各 VPN 服务器的总体设置自带 SNAT 功能，用于 VPN 虚拟网络上外网；VPN 用户也有“用户端口映射”功能，可以实现外网访问 VPN 客户端 OS 的 DNAT 功能。本机各 VPN 客户端的总体设置也自带 SNAT 功能，用于相连的局域网通过 VPN 客户端上 VPN 服务器外网。GRE 隧道也有 DNAT 功能。

4、日志审计

18 种日志，包括系统、管理员、DNS、WEB 代理、IKEv2、OCSERV、PPTP、L2TP、OpenVPN、WireGuard、SoftEther、SS、SSH、防病毒、HIDS、WEBSHELL、WAF、审计日志，均可统计、查询、下载，另外还有内部、WEB 等日志，可以在 SHELL 里查看。无需第三方存储服务，直接留存本机 N 天，方便追溯安全事件。配合 DNS、WEB、SSH 等服务构成真实的 Honeypot 蜜罐。

4.7 网络存储

中神通大地云控系统至少有五种网络存储服务，分别是 WebDAV、NFS、CIFS、SFTP 及 WEBRTC，实时性强，非同步盘，容量、带宽自定义不受限，没有内容审计，没有广告，有用户认证等访问控制，可代替 NAS，可配合本机 VPN 服务一起使用，构建远程超融合系统；可以将本机的各种日志文件放在 WebDAV、NFS、CIFS、SFTP 共享目录里，方便 MSP 等集中审计；可以启用本机防病毒功能，保障文件安全。以下做详细介绍：

1、WebDAV

属于 WEB 服务器的附加网络存储功能，用户可以通过浏览器或挂载为网盘后通过文件管理器进行上传、下载、编辑、增删文件的操作，存储在服务器的文件天然成为 WEB 服务器的网页内容，另外可以配置用户认证做访问控制。部分流媒体播放软件可以实时播放 WebDAV 网络资源，免去了下载存储的过程。WebDAV 没有分用户的容量限制。

使用本机或网络防病毒功能，实现文件系统实时防护。

2、SSH、SFTP

通过专门的客户端软件可以将 SSH、SFTP 服务转化为本地网盘，方便管理远程 Linux 等 OS 的文件系统。SSH、SFTP 有分用户的容量限制。

使用本机或网络防病毒功能，实现文件系统实时防护。

3、NFS

NFS 服务提供基于来源 IP 控制的、没有用户认证但有反向 DNS 查询的网络存储、网盘服务，Linux、MacOS、Windows 客户端可以挂载远程 NFS 资源，用于扩充本地存储空间，和 GD、OD、百度网盘、阿里网盘等同步盘（先本地存储，再上传到网盘）不同，NFS 网盘是数据盘，实时性更强，可即时执行 NFS 网盘内的程序，更接近于本地存储。NFS 没有分用户的容量限制。OpenVZ 系统及 Ucloud CUBE 等容器的内核可能不支持 NFS。

网关、ISP、互联网一般封锁微软的 SMB 网络邻居（137~139、445 端口），但可能不封锁 NFS 网络邻居（111、2049 端口），如果不需要对文件保密，可以直接使用 NFS 共享文件，如果需要对文件保密，可以先 VPN 连接再连接 NFS 资源。

使用本机或网络防病毒功能，实现文件系统实时防护。

4、CIFS

CIFS 服务提供网络存储、网盘服务，Linux、MacOS、Windows 客户端（网络邻居）可以挂载远程 CIFS 资源，用于扩充本地存储空间，和 GD、OD、百度网盘、阿里网盘等同步盘（先本地存储，再上传到网盘）不同，CIFS 网盘是数据盘，实时性更强，可即时执行 CIFS 网盘内的程序，更接近于本地存储。CIFS 没有分用户的容量限制。

由于 ISP、IDC 封杀 139、445 端口，导致无法直接连接 CIFS 资源（文件共享、网络打印机），需要先进行 IKEv2 等 VPN 拨号，再连接 VPN 虚拟网关 IP 的 CIFS 资源，使用本系统即可实现 VPN+网络共享/网络邻居一站式服务，成为一体化远程超融合服务。

使用本机或网络防病毒功能，实现文件系统实时防护。

5、WEBRTC

WEBRTC 可以实现 P2P、去中心化、WEB3.0 即时数据传输服务，局域网用户可直接使用，远程用户需要先通过 VPN 连接，构建虚拟局域网，之后就可以相互聊天或交换文件，具有方便、安全、保护隐私等特点。此服务为收费安装服务。

1）方便

- 免安装软件：只需要浏览器，不需要修改注册表、服务、安全策略、个人防火墙等已有配置，不需要重启；自动兼容安卓、iOS、Windows、Linux 等 OS，可以包装为独立的 APP；可以 P2P 通讯，聊天、传输文件，不需要远程桌面、远程控制；
- 使用时免用户认证：匿名，保护隐私；
- 免服务器存储传输数据：p2p、去中心化，传统还是需要 VPN 服务器的带宽，换成 wireguard mesh vpn，可以真正做到去中心化，VPN 客户端之间的传输也和 VPN 服务器带宽无关；
- 无日志，保护隐私；聊天只显示最后一条信息，自动阅后即焚(最后发送一条无关信息)；
- 连接任意局域网：通过 VPN 连接任意两台异地局域网内的 PC，两个不直接相连的 PC，通过 VPN 服务器中转，做到网络层互联互通，避免 ISP、SNAT

及各自局域网、网关的干扰；甚至不需要互联网，只需要 WIFI、局域网，手机上开一个热点也可以；

IPSEC 的问题：只支持单播流量，组播和广播流量不会穿过数据 SA

- 不需要设置 VPN 为缺省路由，可长期开启 VPN，不会影响正常上网，随机启动、断线重连；

2）安全

- 用户认证：有 VPN 的用户认证；可以共用一个 VPN 账号，可以长期开启 VPN 连接；
- 限制在 VPN 隧道内进行：VPN 隧道加密保护、WEBRTC 等服务器内置在 VPN 隧道里；流量无法被外部监听解密，不存在泄露的风险；
- P2P 传输，没有服务器，就没有 OS、服务器、客户端软件等的安全漏洞，免升级维护；
- 中神通定制化：服务器功能集于一身，一个域名、IP，方便管理，减少外部依赖；更好的判断来源 IP 是否来自同一网络；WEB 服务器具备真实域名的 SSL 证书，可直接访问，免去生成、下载、安装自签名根证书的繁琐；来源 IP 防火墙控制、时间控制

4.8 VPN/SS/SSR/TJ/SSH/IPv6 客户端

开启 VPN/SS/SSR/TJ/SSH/IPv6 客户端既可以为本机提供 VPN/SS/TJ/SSH/IPv6 连通服务(方便本机在线更新 wordpress 插件、git clone https://github.com/user/prj 等)，更可以为局域网或其他用户提供中转服务，其他用户可以通过 VPN 客户端所在系统的 SNAT、WEB 代理服务或 VPN/SS/SSR/TJ/SSH/Socks 服务，间接地连接 VPN 客户端所连接的 VPN 服务器之后的网络，VPN 服务器及其相连的网络也可以连接 VPN 客户端所在的系统及其相连的系统，这样的连接方式类似 WIFI 热点/中继、SD-WAN 的功能，还可绕过 VPN 服务器组成 P2P VPN & Mesh VPN，实现异构网络、异地网络的互联互通。

IKEv2/IPSEC VPN 服务器为多用户的 P2S VPN 服务器，IKEv2/IPSEC VPN 客户端为多个并发的 S2S VPN 端。

以下是几个典型的应用场景。

1）应用场景一

用户有多种移动终端，而且 OS 的版本也不同，可能需要同时连接多个 VPN/IPv6 服务器及网络，逐一安装 VPN 客户端并做设置会十分繁琐，升级维护也不方便，而且容易造成用户名口令泄密，为此可以设立一台前置/中转服务器，在其上启用相应的 VPN 客户端以及 SNAT 或带用户认证功能的 WEB 代理服务器，用户只需要通过单一的用户认证连接上 WEB 代理服务器，就可以同时连接多个 VPN 服务器及网络。以 SNAT 为例，局域网 PC 可以直接以路由的方式通过这台 VPN 客户端访问其后的 VPN 网络——而不需要 VPN 拨号，只是需要另外设置路由，可以由 PC 自己设置，也可以由局域网网关设置。由此，可以将点到站/网到网（Point to Site/P2S）VPN 转化成站到站（Site to Site/S2S）VPN，方便 VPN 部署，我们称之为 VPN 前置机或 VPN 中转机。

2）应用场景二

本地因网络阻隔、出口 IP 随机、QoS 限制或没有配对的 VPN 客户端不方便直接连接异地的网络，而国内其他地点可以无限制地连接异地的网络，为此可以在国内其他地点（VPS）上部署本系统启用 VPN/SSH 客户端，连接异地的 VPN/SSH 服务器（正向代理穿透）或者启用异地的 VPN/SSH 客户端，连接国内 VPS 的 VPN/SSH 服务器（反向代理穿透），本地用户就可以通过国内 VPS 上的 HTTP/Socks 代理服务或 VPN/SS/TJ/SSH 服务连接异地的网络。本机所在 IDC 对 DNS 查询做过滤，无法使用特定的 DNS 服务器，为此可以通过本机 VPN 客户端连接远程网络，VPN 路由仅仅是特定的 DNS 服务器即可

3）应用场景三

写字楼里，单位网络处在 NAT 内网里，而且无法在 NAT 路由器上做端口映射，外界无法直接连接单位边界路由器或服务器，为此可以在国内其他地点（VPS）上部署本系统并启用 VPN 服务器，让移动客户端和单位服务器作为 VPN 客户端同时连接到这台 VPN 服务器上，并让 VPN 客户端之间互相连通（客户端代理穿透），这样就可以实现移动客户端和单位服务器之间的连接；或者在单位（VPN）服务器上启用 VPN/SSH 客户端，连接国内 VPS 的 VPN/SSH 服务器（服务器代理穿透），移动客户端就可以通过国内 VPS 上的 HTTP/Socks 代理服务或

VPN/SS/TJ/SSH 服务连接单位(VPN)服务器。传统的硬件 VPN 路由器没有 VPN/SSH 客户端功能，无法解决上述问题。

4）应用场景四

本地无法直接使用 8.8.8.8 作为 DNS 服务器，无法查询 IPv6 域名，为此可以在国内 VPS 上部署本系统，并将 8.8.8.8 作为 VPN 客户端的 VPN 路由以及该机的 DNS 服务器，同时启用 DNS 代理服务，本地用户就可以将该国内 VPS 的 IP 作为 DNS 服务器，间接使用 8.8.8.8 进行 DNS 查询，由于经过的是 VPN 隧道，因此也没有大型节点处的 DNS 劫持或 DNS 污染。

5）应用场景五

用户现使用 SOHO 型路由器，在其上安装插件或者定制化的 OS 连接远程 VPN/SS/SSH 服务器，使得内部局域网所有设备都能通过路由器连接远程网络，但受到硬件性能、可用性及部署位置的影响，存在性能不高、带宽不够、维护麻烦、没有访问控制、没有日志留存、不能全方位（局域网、移动网络及互联网）接入、宕机后影响整个网络等问题，为此可以将 VPN/SS/SSR/TJ 客户端以及 WEB/DNS/VPN 服务器功能移出路由器，在更好的 x86 硬件或云主机上安装本系统，接入更大的带宽，用户再通过 WEB/Socks 代理服务（具备广告等 20 多种域名库过滤、自定义域名过滤、URL 过滤以及日志审计留存等功能)或 VPN/SS/TJ/SSH 服务连接到该系统上，从而完全克服上述这些问题。另外，SOHO 型路由器自身没有大容量存储空间，无法作为网络存储服务器，而 VPS 可以挂载大容量存储器，适合作为网络存储服务器。

6）应用场景六

用户有多个 X86 或 VPS 主机需要相互连接，为此可以选择一台带宽大性能好的服务器，开启 VPN 服务，并绑定用户名和虚拟 IP，其它主机开启 VPN 客户端，经过用户认证连接到这台服务器，并根据需要打开或关闭客户端防火墙，这样各主机之间就可以在一个加密的虚拟网络里相互通信，共享文件和网络服务。

7）应用场景七

用户有多个 X86 或 VPS 主机没有原生的 IPv6 IP，可以通过 OpenVPN/IPv6 隧道客户端获得 IPv6 IP，使得本机甚至在局域网内（内网穿透）也能够为 IPv6 网络提供各种内置服务，为满足苹果 iOS APP IPv6-only 等测试提供帮助，还可以运行

本机其它 VPN/SS/SSH/BT 等客户端连接 IPv6 服务器，例如北邮人、六维等 IPv6 PT。

5、IPv6 接入及 GRE 隧道

5.1 IPv6 功能

5.1.1 IPv6 接入方式

原生 IPv6

ISATAP 接入

Teredo 隧道接入

HE 隧道接入：Linux 下有 WEB GUI 设置及状态监控界面；有用户和内核两种驱动，可以为有公网 IPv4 的 VPS 安装上 IPv6 IP

OpenVPN 客户端接入：Linux 下有 WEB GUI 设置及状态监控界面；Windows 下有可定制的 GUI 客户端软件

获得 IPv6 IP 后，可以通过 DDNS 客户端，将 IPv6 IP 映射为好记的域名。

5.1.2 禁用 IPv6

IPv6 总体开关

OS 级 IPv4、IPv6 优先选择

DNS 服务器-启用“过滤 AAAA 查询”功能

WEB 代理服务器-停用“域名 IPv6 解析优先”功能

5.1.3 防火墙及流量统计

基于 IPv4 IPv6 双栈的 Iptables 防火墙模板

基于 IPv4 IPv6 双栈的 fail2ban 防暴力破解用户名密码

显示各服务的 IPv6 IP 地址的监听状态

显示各服务的 IPv6 IP 地址的流量统计

5.1.4 测试工具

ping6 IPv6 IP 地址

traceroute6 IPv6 IP 地址

nslookup AAAA 解析 IPv6 IP 地址

whois IPv6 IP 地址

telnet IPv6 IP 地址 端口

5.1.5 IPv6 hosts 文件

Google IPv6 hosts：无需其它软件，只需要设置用户 URL、在线代理或代理服务器，使用户上 IPv6 网络；定时自动更新 IPv6 解析

可自定义 IPv6 hosts

5.1.6 DNS 服务器

启用、停用“过滤 AAAA 查询”功能

本机可设置 IPv6 DNS 服务器，使用 DNS64、NAT64 服务器可以为纯 IPv6 网络环境提供访问 IPv4 网络的能力

本机可设置非标准端口 DNS 服务器获得无污染 IPv6 IP 解析

监听 IPv6 IP 地址，接受 IPv6 客户端访问

自主管理 NS 域名可以设置 AAAA 记录

DDNS 客户端可以设置 AAAA 记录

日志记录中包含 AAAA 类型

源 IP 控制可以是 IPv6 IP 网络

5.1.7 WEB 服务器

监听 IPv6 IP 地址，接受 IPv6 客户端访问，获取 IPv6 网络资源

在线代理支持访问 IPv6 IP 地址以及 hosts 中定义的 IPv6 域名

WebDAV 访问支持 IPv6 访问

用户 URL 支持 IPv6 IP 地址：

1）HTML 跳转、302 跳转、反向代理、在线代理（单个元素）、在线代理

2）公网 IPv6 映射到 VPN 客户端虚拟 IP

提供显示客户端 IPv6 IP 地址、探针、网络测速的在线服务

SFTP WEB 在线客户端，让 IPv4/IPv6 用户访问 IPv6/IPv4 主机

源 IP 控制可以是 IPv6 IP 网络

通过 IPv6 网络申请真实域名 SSL 证书，网站不需要备案

5.1.8 WEB 代理服务器

监听 IPv6 IP 地址，接受 IPv6 客户端访问，获取 IPv6 网络资源

双栈网络中，接受 IPv4 客户端访问 IPv6 网络，指定 IPv6 为出口 IP（上 NF）

双栈网络中，接受 IPv6 客户端访问 IPv4 网络

启用、停用“域名 IPv6 解析优先”功能，优先访问 IPv6 IP 地址

来源 IP、目的 IP 策略可以过滤 IPv6 IP 地址

例外的域名白名单中可以有 IPv6 IP 地址

5.1.9 VPN/SS/TJ/SSH 服务器

监听 IPv6 IP 地址，接受 IPv6 客户端访问，获取 IPv6 网络资源

提供虚拟 IP SNAT 服务，为 IPv4/V6 网络互联互通搭桥

下发给客户端的网络可以是 IPv6 IP 网络

下发给客户端的 DNS 服务器可以是 IPv6 IP 地址

SSH 服务可以提供正向、反向端口映射及 SOCKS 代理，方便 IPv4/V6 网络互联互通

日志记录中包含 IPv6 IP 地址

源 IP 控制可以是 IPv6 IP 网络

5.1.10 VPN/SS/SSR/SSH 客户端

连接 IPv6 服务器地址

连接 IPv4 VPN 服务器得到 IPv6 虚拟 IP 地址，为 IPv4/V6 网络互联互通搭桥

将 IPv6 服务映射到 IPv4 网络，为 IPv4/V6 网络互联互通搭桥

将 IPv4 服务映射到 IPv6 网络，为 IPv4/V6 网络互联互通搭桥

客户端 VPN 网络可以是 IPv6 IP 网络

源 IP 控制可以是 IPv6 IP 网络

5.1.11 应用服务

Stunnel、TLSProxy、KMS、BT、NFS、CIFS 等应用服务

5.1.12 管理界面

IPv6 服务器地址的 WebAdmin 管理界面

IPv6 服务器地址的 WEB 用户门户

5.2 IPv6 用途

5.2.1 "IPv6 用户"上 IPv6 网络

原生 IPv6

ISATAP 接入

Teredo 隧道接入

HE 隧道接入：Linux 下有 WEB GUI 设置及状态监控界面；有用户和内核两种驱动，可以为有公网 IPv4 的 VPS 安装上 IPv6 IP

OpenVPN 客户端接入：Linux 下有 WEB GUI 设置及状态监控界面；Windows 下有可定制的 GUI 客户端软件

5.2.2 IPv4 用户上"IPv6 网络"

WEB 在线代理

WEB 代理

SS、TJ 服务器

SSH 服务器

VPN 服务器

Stunnel、TLSProxy、KMS、BT、NFS、CIFS 等应用服务

5.2.3 IPv6 用户上"IPv4 网络"

WEB 在线代理

WEB 代理

SS、TJ 服务器

SSH 服务器

VPN 服务器

Stunnel、TLSProxy、KMS、BT、NFS、CIFS 等应用服务

5.2.4 IPv6 用户访问"IPv4 服务器"

DNS 服务器-过滤 AAAA 查询

DNS64、DNS64 客户端

WEB 在线代理

WEB 代理

SS、TJ 服务器

SSH 服务器

VPN 服务器

SFTP WEB 在线客户端，可 IPv6 用户访问 IPv4 主机

5.2.5 IPv4/V6 用户访问"IPv6 服务器"

WEB 在线代理

WEB 代理-域名 IPv6 解析优先

SS、TJ 服务器

SSH 服务器

VPN 服务器

SFTP WEB 在线客户端，可 IPv4/v6 用户访问 IPv6 主机

不受源 IP 限制，使用 CloudFlare Gateway 等 IPv6 DNS 服务

5.2.6 获得无污染的"IPv6 域名"

Google IPv6 hosts：无需其它软件，只需要设置用户 URL、在线代理或代理服务器，使用户上 IPv6 网络；定时自动更新 IPv6 解析

DNS 代理服务器：非标准端口 DNS 服务器；IPv6 DNS 服务器

5.2.7 不受备案限制申请 SSL 证书

通过 IPv6 网络申请真实域名 SSL 证书，网站不需要备案

5.2.8 内网穿透

为局域网机器分配公网 IPv6 IP，方便局域网机器之间及公网用户连接

5.2.9 禁用 IPv6 网络

防止来自外部 IPv6 网络中的恶意攻击，避免 IPv6 地址泄露，避免 IPv6 网络网速慢

5.3 GRE 隧道

5.3.1 GRE 隧道功能

GRE 隧道是 OS 内核通过 GRE 协议（protocol 47）建立的虚拟路由隧道，无需第三方服务提供商也没有服务进程，只需要有公网 IP 的两台主机或路由器等网

络设备即可互联互通，有 GRE 和 IPIP 两种子类型。传统 GRE 隧道一般由路由器、防火墙、网关实现，大地云控的 GRE 隧道是在主机上实现的，相当于集成了一台路由器，主要是为了发布主机自身的服务，当然也可以用作网关连接两个内网。

GRE 隧道建立后

I）主机将获得一个虚拟 IP，双方通过虚拟 IP 通讯；如果是在两个网关上做 GRE 隧道，则两个网关连接的两个内网还可以通过虚拟 IP 做目的路由互通

II）可以启用 DNAT 端口映射功能，将对端主机某一应用服务的端口映射到本机的某一端口上，可以保护对端主机的 IP 信息，防止被扫描攻击，还可用于中转被网络隔离的主机。

GRE 隧道没有加密，为了保密，请在 GRE 隧道中使用 https 等加密的应用；如果需要全程加密、用户认证或者主机没有公网 IP，请使用 OpenVPN、IKEV2 等 VPN；当传统的 VPN 被阻拦或 QoS 限流时，可以使用 GRE 隧道建立虚拟路由达到使用 VPN 一样的效果。

5.3.2 GRE 隧道应用

I）可以直接使用远端的 WEB 服务器或结合本地 WEB 服务器的反向代理功能，将远程 WEB 应用映射为本机 WEB 服务的一个分支 URL，这样可以利用本机的外网 IP、域名、SSL 证书、域名备案、WAF、抗 DDoS 攻击等资源，同时保护远端主机的 IP 地址等信息，防止被扫描攻击；

II）可以使用 WEB 服务器的在线代理或 WEB 代理服务器功能，以对端主机的外网 IP 进行浏览，可用于中转被网络隔离的主机；

III）可以使用 DNS 代理服务器，在远程主机的网络中进行域名解析，避免 DNS 污染、DNS 劫持

6、软件安装

1）软件下载

中神通大地云控提供安装软件下载及 OS 镜像文件下载，安装软件可以在主流 Linux OS 中安装使用，TRUSTGATE-ROM/VM 镜像文件作为 X86 硬件/虚拟机的 OS，可以使 X86 硬件/

虚拟机一步到位升级为一台具备 VPN、NAT、防火墙、IPv6、DNS、WEB、代理、存储等诸多功能的硬件安全网关/虚拟服务器。

最新下载信息：http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1174

中神通公司另有大地云控 TrustGate 硬件网关设备发售，可作为 SOHO/SMB 级（NAT、VPN、上网行为管理）路由器/安全网关使用，并提供 OEM/ODM 服务。

详见：http://www.trustcomputing.com.cn/cn/index.php/product/appliance/125-trustgate

2）文档下载

1、中神通大地 EDR&DNS&URL&VPN 云控管系统-系统简介

TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System - Brief Introduction

http://www.trustcomputing.com.cn/help/zst_dadi_intro.pptx

2、中神通大地 EDR&DNS&URL&VPN 云控管系统-系统介绍

TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System - Introduction

http://www.trustcomputing.com.cn/help/zst_dadi_intro.docx

3、中神通大地 EDR&DNS&URL&VPN 云控管系统-功能列表

TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System – Function List

http://www.trustcomputing.com.cn/help/zst_dadi_func.doc

4、中神通大地 EDR&DNS&URL&VPN 云控管系统-管理员手册

TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System - Administrator's Guide

http://www.trustcomputing.com.cn/help/zst_dadi_adm.doc

5、中神通大地 EDR&DNS&URL&VPN 云控管系统-用户指南

TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System - User's Guide

http://www.trustcomputing.com.cn/help/zst_dadi_userguide.pdf

6、客户端设置一览表

TrustComputing DADI EDR&DNS&URL&VPN Cloud Control System – Client Setup List

http://www.trustcomputing.com.cn/help/client_setup_list.docx

3）技术说明

1、中神通大地云控官网

TrustComputing DADI official website

http://www.trustcomputing.com.cn/cn/index.php/product/dns-url

2、中神通大地云控产品类型对比说明

Comparison of product types of TrustComputing TrustGate

http://trustcomputing.com.cn/cn/index.php/product/compare/126-alldadi

3、中神通大地云控、VPN、SD-WAN、SASE 比较

Comparison of TrustComputing TrustGate, VPN, SD-WAN and SASE

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1763

4、云市场 VPN 商品比较

Comparison of VPN products in cloud market

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1825

5、Darkside 勒索病毒的网络防御措施

Network defense measures against Darkside virus

http://trustcomputing.com.cn/cn/index.php/support/techdocs/121-anti-darkside

6、零信任 VPN 系统

Zero trust VPN system

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1592

7、运用 Mesh VPN 自建去中心化网络基础设施服务

Self built decentralized network infrastructure services using mesh VPN

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1820

8、运用中神通大地云控组建 Mesh VPN 网络

Establish mesh VPN network by using TrustComputing TrustGate

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1821

9、运用 WireGuard 构建下一代内核级 VPN

Using wireguard to build the next generation kernel VPN

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1741

10、安装和管理大地云控系统的视频演示

Video demonstration of installation and management of TrustComputing TrustGate

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1175

11、用户使用大地云控的视频演示、客户端软件及使用说明

Video demonstration, client software and instructions for users to use TrustComputing TrustGate

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1176

12、中神通大地云控思维导图

Mind map of TrustComputing TrustGate

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1266

13、中神通大地云控 IPv6 说明

Description of TrustComputing TrustGate's IPv6 function

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1406

14、如何让 Windows 网络邻居安全的在云上复活？

How to make windows network neighborhood safely revived in the cloud?

http://trustcomputing.com.cn/bbs/viewthread.php?tid=1668

15、中神通大地云控 WEB 服务器自定义 URL 功能介绍

Introduction of custom URL function of TrustComputing TrustGate's WEB Server

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1478

16、大地云控与传统 DDNS、内网穿透相比的特点和优势

The characteristics and advantages of TrustComputing TrustGate compared with traditional DDNS and LAN penetration

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1543

17、大地云控基于 GRE 隧道+端口映射的公网穿透

Public network penetration of TrustComputing TrustGate based on GRE tunnel + port mapping

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1611

18、中神通大地云控的流量统计、控制、计费、运营功能介绍

Introduction of traffic statistics, control, billing and operation functions of

TrustComputing TrustGate

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1581

19、中神通大地云控-TOTP 动态密码认证设置及使用过程

Setting and using process of TOTP dynamic password authentication of TrustComputing TrustGate

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1562

20、中神通大地云控-VPN 端口映射设置及使用过程

VPN port mapping setting and using process of TrustComputing TrustGate

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1561

21、安卓系统在 4G 移动数据流量及 WIFI 时设置（DOT 加密）DNS 服务器

Android system in 4G mobile and WiFi setting (DOT encryption) DNS server

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1631

22、在 Docker 容器中安装使用中神通大地云控系统

Installing and using TrustComputing TrustGate system in docker container

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1606

23、在公有云云市场中使用大地云控 OS 镜像的注意事项

Considerations for *Using TrustComputing TrustGate OS image in public cloud market*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1540

4）在线演示

https://47.99.186.118:999 （因备案问题无法使用域名，https://demo.trustcomputing.com.cn:999）

用户名：adm 密码：utmwall99


中神通 大地云控
Make Cloud Better


中神通
TrustComputin