**运用WireGuard构建下一代内核级VPN**

**Building next generation kernel VPN with WireGuard VPN**

**本文链接：**http://trustcomputing.com.cn/help/wireguard\_zstdadi.docx

## 一、现有主流VPN特性

目前市场主流的VPN有IPSEC VPN、SSLVPN、PPTP VPN、L2TP VPN等，它们在安全性、性能等方面都存在明显的缺点，具体见下表1所示。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 端口、内核级 | 安全性 | 性能 | 复杂度 | 可续性 | 其它特性 | 推荐指数 |
| IPSEC VPN | 500/UDP  4500/UDP  ESP  非100%内核级 | 高 | 一般 | 极高 | 一般 | 端口及协议固定，容易被封；  配置复杂，对管理员要求高；  Windows、iOS没有内置客户端，不适合移动客户 | ✯✯✯ |
| SSLVPN | 443/TCP  非内核级 | 一般 | 差 | 高 | 一般 | 基于WEB浏览器的SSLVPN经常爆安全漏洞，而且性能差；  主流OS没有内置客户端，不适合移动客户 | ✯✯ |
| PPTP VPN | 1723/TCP  GRE  非内核级 | 差 | 一般 | 一般 | 无 | 原理上有安全缺陷；  端口及协议固定，容易被封；  主流OS有内置客户端，适合移动客户 | ✯✯ |
| L2TP VPN | 1701/UDP  非内核级 | 差 | 一般 | 一般 | 无 | 原理上有安全缺陷；  端口及协议固定，容易被封 | ✯✯ |

**表1 主流VPN特性**

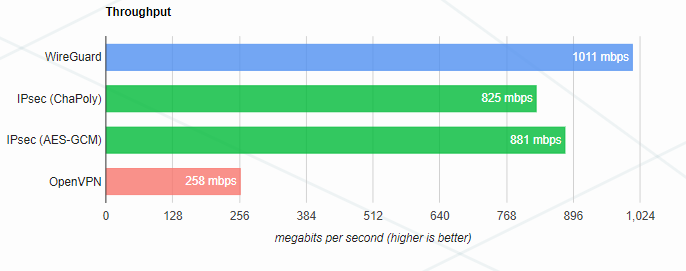
## 二、WireGuard VPN介绍

WireGuard VPN是最新开发的内核级VPN，被Linux创始人Linus Torvalds极力推荐，并于2020年1月正式合并进了Linux 5.6内核，之后，Google也将WireGuard VPN添加到安卓12的Linux内核中，它的优点是安全性高、性能高、复杂度低，具体见下表2所示。

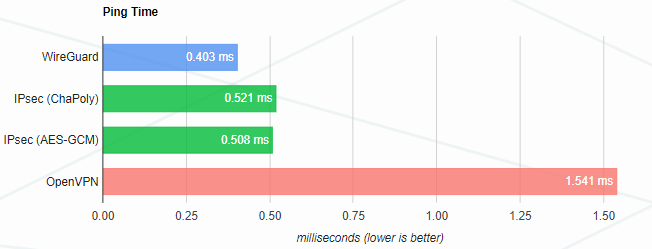
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 端口、内核级 | 安全性 | 性能 | 复杂度 | 可续性 | 其它特性 | 推荐指数 |
| WireGuard VPN | 不固定端口/UDP  100%内核级 | 高 | 高 | 低 | 高 | 端口不固定，不容易被封；  没有动态IP分配机制，只能事先指定用户的虚拟IP；  命令行配置较麻烦，缺少日志等配套措施 | ✯✯✯✯ |

**表2 WireGuard VPN特性**

WireGuard VPN直接在内核层面处理路由，直接使用系统内核的加密模块来加密数据，省去了用户进程和内核交互的开销，因此性能优越，具体表现为吞吐量高，是SSLVPN/OpenVPN的2~4倍，见图1所示，同时，时延低，是SSLVPN/OpenVPN的30%~40%，见图2所示。



**图1 主流VPN吞吐量比较**



**图2 主流VPN时延比较**

对于100~10000用户数的VPN、零信任、SASE、SD-WAN系统，吞吐量、时延都是必须考虑的关键性能指标。内核处理意味着系统负载小，可长期稳定运行；吞吐量越大意味着在相同带宽下并发用户数越大，投入产出比越高；时延越小意味着信息处理速度越快，工作效率越高，其重要性可参考电影《蜂鸟计划》。

判断VPN服务是否是100%内核处理，可以通过在SHELL下运行netstat –nap命令，查看VPN服务器监听端口所对应的程序，如果最后一列有程序名，就表示是用户态程序监听，如果最后一列是“-”没有程序名，就表示是内核亲自在监听，以下对大地云控系统内的各种VPN服务器进行统计，具体见下表3所示。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 端口及协议 | 监听程序 | 100%内核处理 |
| IKEv2/IPSEC VPN | 500、4500/UDP | charon | 否 |
| SSLVPN | 443/TCP | ovpnd | 否 |
| PPTP VPN | 1723/TCP | pptpd | 否 |
| L2TP VPN | 1701/UDP | l2tpd | 否 |
| CISCO OCSERV VPN | 43/UDP | ocserv-main | 否 |
| Softether/SSTP VPN | 5566/TCP | vpnserver | 否 |
| WireGuard VPN | 52021/UDP | - | **是**  （需内核支持） |

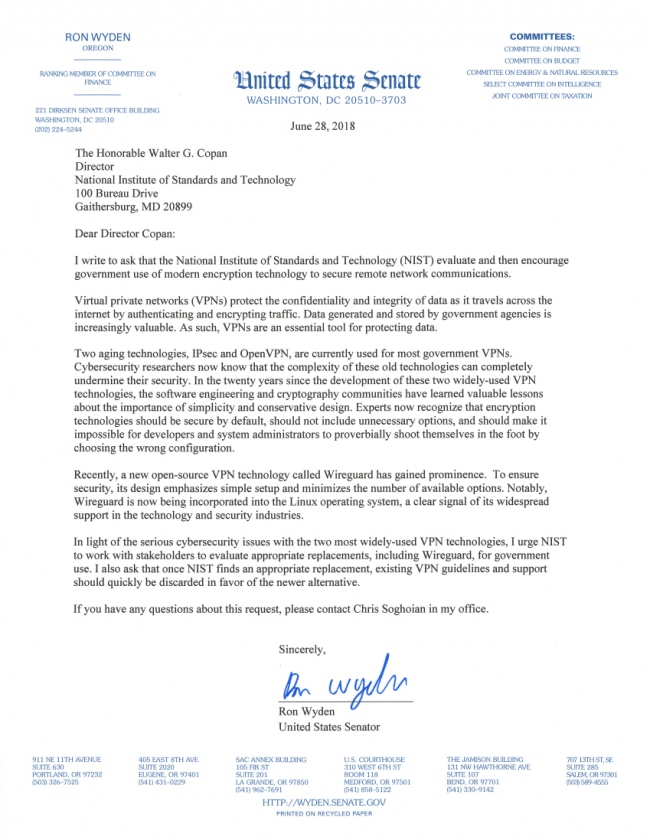
**表3 大地云控系统内的各种VPN服务器的监听程序统计**

WireGuard VPN使用UDP协议，避免了TCP协议的三次握手；对于未认证的数据包直接丢弃，外界无法探测端口的存在性；没有数据传输时，不产生网络流量。这些特性使得WireGuard服务器在网络中隐形，符合零信任安全架构对服务器的要求。

WireGuard VPN只有几千行核心源代码，被Linus称为“艺术品 (Work of art)”，不到IPSEC VPN、OpenVPN/SSLVPN源代码的1%，这意味着容易审计，出错的机率低，可持续性好。

WireGuard VPN内置了最新的加密算法组合，用户0配置，既保证了安全性又降低了用户配置的难度，即降低了用户配置错误的概率。

为此，2018年6月美国俄勒冈州参议员Ron Wyden向美国国家标准与技术研究所NIST推荐WireGuard VPN，用来代替美国政府使用的、老旧的、容易出错的IPSEC VPN和OpenVPN/SSLVPN，见下图3所示。



**图3 美国俄勒冈州参议员向NIST推荐WireGuard VPN**

从以上说明可以看出，自2020年起，现有的IPSEC VPN、SSLVPN、PPTP VPN、L2TP VPN终将被WireGuard VPN所代替，VPN将进入一个全新发展的阶段。

## 三、大地云控WireGuard VPN模块介绍

中神通大地DNS&URL&VPN云控管系统（简称大地云控）是一套互联互通安全服务器软件，可将硬件、虚拟化平台打造为IPv4/IPv6双栈分布式云路由器，将公有云、私有云、行业云打造为云接入安全网关（Cloud Access Security Gateway/Security Access Services Edge），将IaaS及软件网络资源升级为SaaS。大地云控集成有7种VPN服务器和8种VPN客户端，包括IKEv2/IPSEC VPN、CISCO OCSERV VPN、PPTP VPN、L2TP VPN、OpenVPN/SSLVPN、WireGuard VPN、SoftEther VPN/SSTP VPN等，**是目前最全的VPN系统**。其中，WireGuard VPN服务器可同时连接多个客户端，并为客户端提供DNAT端口映射及URL映射反代服务，同机的WireGuard VPN客户端又可同时连接多个服务器（多云），并为其所在局域网提供到VPN路由的SNAT服务，还都可以和应用系统共处一机，由此，**可以实现万物互联——连接任意类型的网络，构造任意复杂的网络**。

WireGuard VPN是公钥/私钥加密体制，加密参数由自己的私钥和对方的公钥组成，即通讯双方需要事前交换公钥，服务器的公钥一般是公开的、固定的，比较麻烦的是用户公钥的处理，要能自动生成用户的密钥对——公钥私钥，每一个用户的公钥要上传到服务器上，服务器的配置文件要能及时更新。当客户端数量大时，密钥的生成、修改、销毁和交换，以及客户端配置文件的获取成为了一种管理负担（与之相对应，IKEv2 VPN是CA加密体制，如果使用真实域名的CA证书，可以免去事前交换公钥这一步，中神通大地云控可自动申请、维护CA证书，同时也有自定义CA证书），为此中神通大地云控于2020年12月（国内/国际/全球）独家推出了WireGuard VPN模块，对WireGuard VPN的管理做了各方面的完善，让WireGuard VPN能真正走向实用，具体功能见下所示。

**3.1 WireGuard VPN总体设置**

提供内核级及用户态两种运行方式，设置WireGuard VPN监听端口、启用停用SNAT、虚拟IP地址池、目的IP地址池、源IP控制、时间控制、流量控制、服务器公钥私钥、客户端DNS服务器等，自动生成Iptables网络防火墙规则，定期检查、修复WireGuard VPN状态（Watchdog），根据公网IP、服务器公钥更新已有客户端配置文件，管理界面见下图4所示。



**图4 WireGuard VPN总体设置管理界面**

**3.2用户管理**

提供用户账户的增删改功能，用户账号可设置有效期（绝对日期或相对时长），可进行流量统计及控制，可使用发卡系统分配账号，可强制用户登录WEB用户门户，可设置反向DNAT端口映射策略（内网穿透）。新建用户时，自动生成公钥私钥，自动生成虚拟IP；新建、修改用户时，自动生成WireGuard VPN客户端配置文件，自动生成配置文件的二维码图片。管理界面见下图5所示。





**图5 用户设置管理界面**

**3.3用户状态**

显示曾经登录过的用户状态信息，包括用户账号、远程IP、虚拟IP、上一次活动的时间、上传下载流量统计等，管理界面见下图6所示。



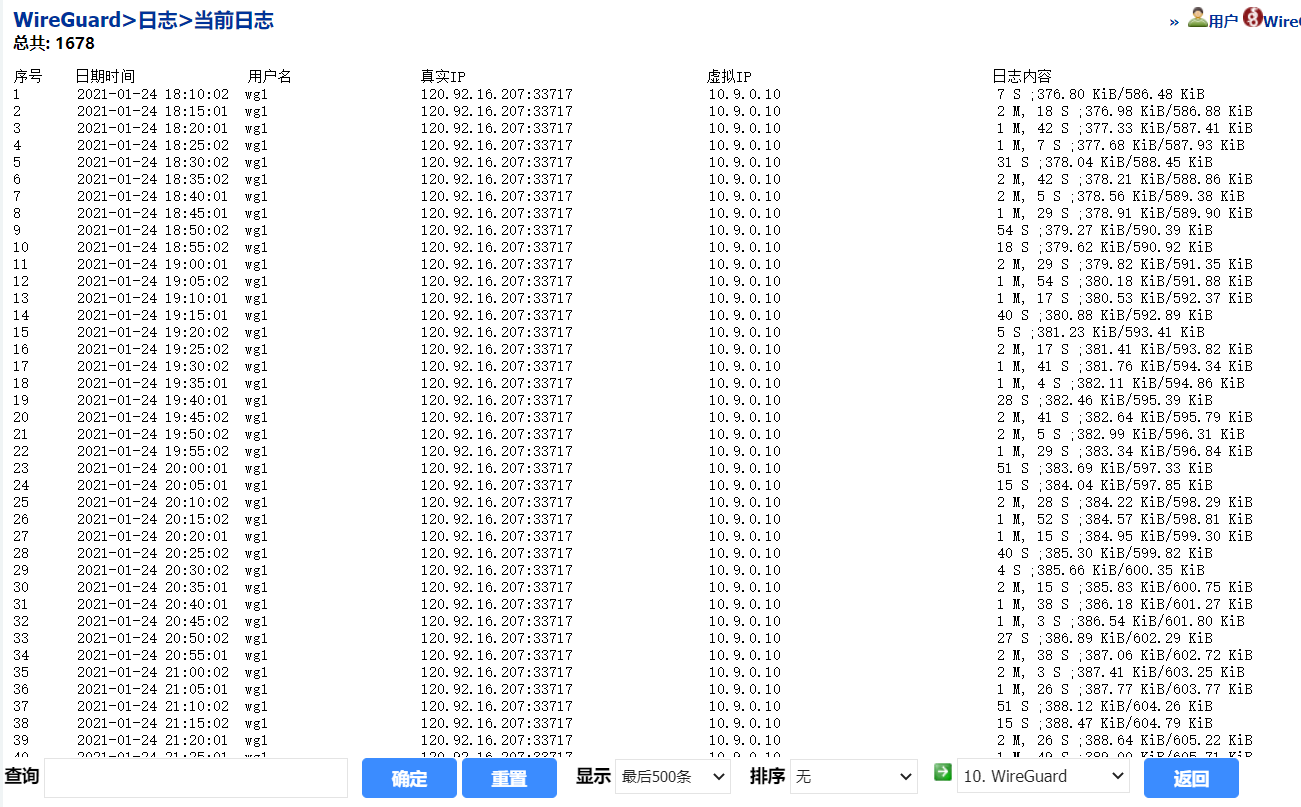
**图6 用户状态管理界面**

**3.4用户日志**

对用户登录状态做日志留存、日志统计、日志查询，方便事后监管，管理界面见下图7所示。







**图7 用户日志管理界面**

**3.5用户门户**

为终端用户提供自服务WEB用户门户，用户登录后强制修改密码，下载WireGuard VPN客户端配置文件、扫描配置文件的二维码，修改、更新、销毁WireGuard VPN公钥私钥，查看账号状态、有效期，查看可用资源，查看对外服务项目，查看公告等。有了自服务WEB用户门户，成百上千用户WireGuard VPN密钥的分发、修改、销毁不再是管理负担，用户门户界面见下图8所示。







**图8 用户门户界面**

**3.6内置DNS**

无需第三方DNS服务器，为内部应用系统提供域名解析服务；避免VPN使用过程中的DNS泄露，实现VPN隧道内域名过滤和日志留存及审计，有大规模域名库和自定义域名规则等控制措施，管理界面见下图9所示。





**图9 DNS服务器管理界面**

**3.7 Linux WireGuard VPN客户端**

提供Linux WireGuard VPN客户端拨号功能，可同时连接多个IPv4/IPv6服务器（多云），Windows、安卓、iOS等系统的客户端软件缺省只能同时连接一个服务器。可利用WARP等服务资源，为IPv6主机提供IPv4 IP，使得本机可访问IPv4资源，同时IPv4用户可访问本机；也可以为IPv4主机提供IPv6 IP，使得本机可访问IPv6资源，同时IPv6用户可访问本机。可启用停用客户端防火墙，VPN连接成功后，为本机设置VPN路由，同时可以为局域网其它设备（不用安装VPN客户端软件）提供到VPN路由的SNAT服务，由此可实现网到网（Site to Site）VPN及VPN链（与本机WireGuard VPN服务器不同的虚拟IP地址）等高级应用，管理界面见下图10所示。



**图10 Linux WireGuard VPN客户端管理界面**

**3.8管理员及用户使用文档**

**1、用户指南**

* 中神通大地EDR&DNS&URL&VPN云控管系统-管理员手册

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

http://www.trustcomputing.com.cn/help/zst\_dadi\_adm.doc

* 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

**2、视频演示**

* WireGuard VPN管理员设置

http://www.trustcomputing.com.cn/help/cn/dadi/wireguard/wireguard\_admin.html

* Windows安装使用WireGuard VPN软件

http://www.trustcomputing.com.cn/help/cn/dadi/wireguard/windows\_wireguard.html

* 安卓系统安装使用WireGuard VPN APP

http://www.trustcomputing.com.cn/help/cn/dadi/wireguard/android\_wireguard.html

## 四、WireGuard VPN部署流程

使用大地云控部署WireGuard VPN系统的流程简述如下，也可参见下图11所示。

1）管理员启用WireGuard VPN，参见3.1总体设置

2）管理员新建用户，参见3.2用户管理

3）管理员亲自下发配置文件及客户端软件给用户；或者，用户自行登录用户门户下载配置文件及客户端软件，参见3.5用户门户

4）用户安装VPN客户端软件，导入配置文件，连接VPN服务器

**图11 WireGuard VPN部署流程示意图**

管理员下载配置文件、二维码和VPN客户端软件一起分发给用户

3.2用户管理

用户登录门户，自行下载VPN客户端软件及配置文件、二维码

3.5用户门户

管理员新建用户

3.2用户管理

管理员启用WireGuard VPN

3.1总体设置

用户安装VPN客户端软件，导入配置文件，连接VPN服务器

## 附录

中神通大地云控官网：http://trustcomputing.com.cn/cn/index.php/product/dns-url

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

零信任VPN系统： http://trustcomputing.com.cn/bbs/viewthread.php?tid=1592