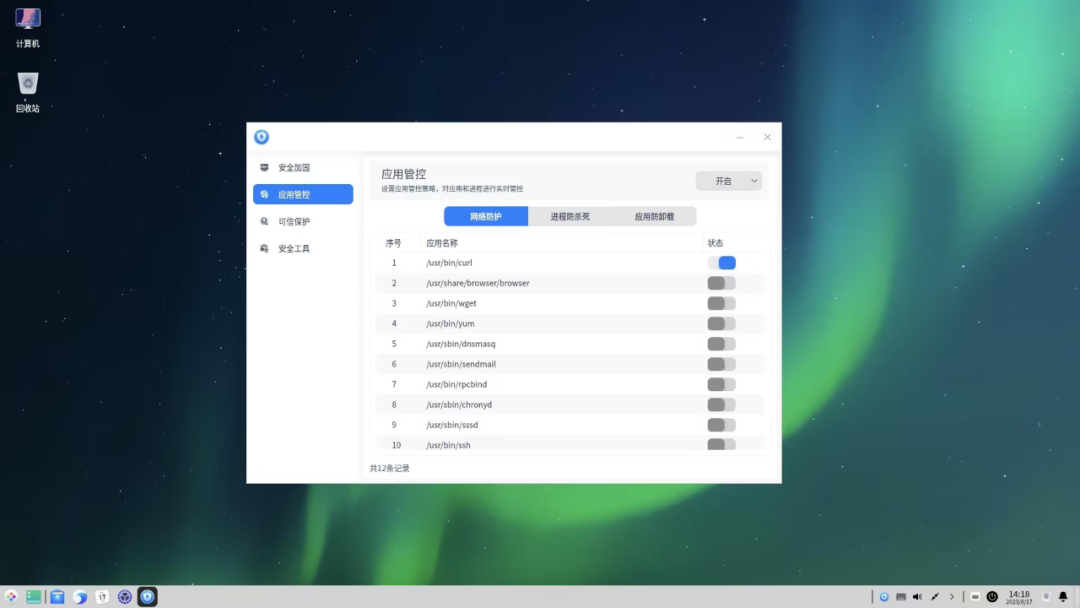


6月初，统信UOS服务器版V20（1060）盛大推出，不仅带来了突破性的功能和性能提升，还带来了统信UOS系统安全软件（简称「统信有固」）的安全“配方”再升级，为服务器操作系统的稳定运行提供更加强大的安全保障。

最新消息：「统信有固」将于近期推出全新的应用层网络管控方案，旨在让客户使用统信UOS时享受更安全、更高效、更稳定的网络体验。



该方案通过结合先进且强大的网络技术，不仅能够实时监控网络应用，还能按需设置网络应用的带宽和流量，大大提升网络应用的可管理性。

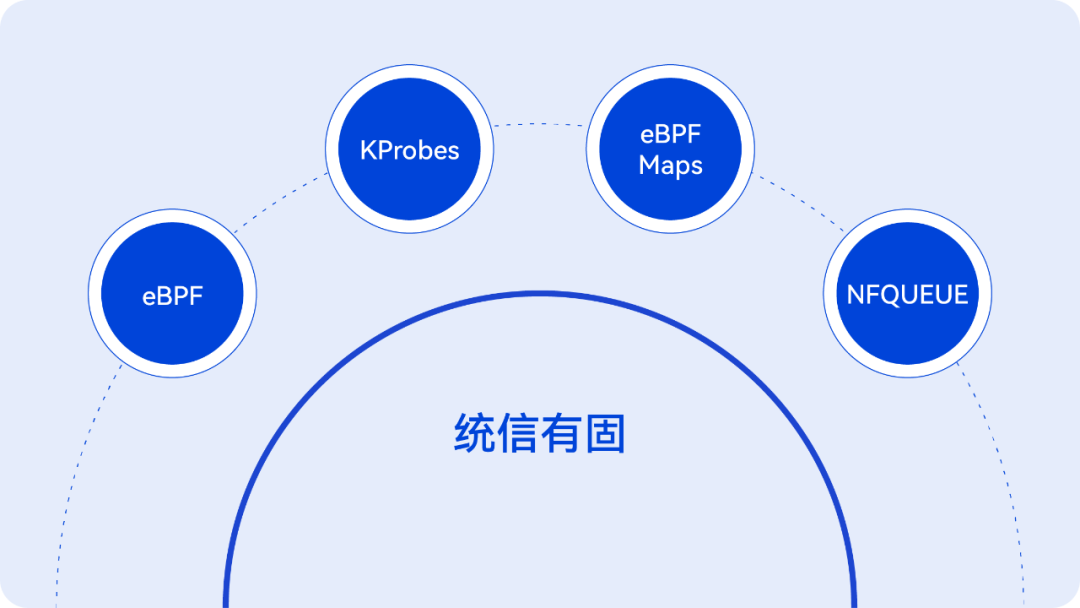
**统信有固**

统信UOS服务器版V20的安全加固和配置工具，「统信有固」在全栈系统安全防护体系中扮演着重要的角色，提供了系统安全加固、完整性度量、应用管控、可信保护、三权分立等功能，保障系统的安全稳定运行。

创新方案：必然趋势

随着网络应用的飞速发展，Linux中关于应用层网络管控方面的需求也日益增加。

然而，传统的网络管控工具，如iptables、firewalld等，很难针对应用层进行网络管控。因此，创新性的应用层网络管控方案成为必然的发展趋势。



「统信有固」通过引入eBPF、KProbes、eBPF Maps、NFQUEUE技术，构建了一种全新的应用层网络管控方案，能够实时监测和管理应用层网络。

火爆技术：引入瞩目

▶eBPF

eBPF（Extended Berkeley Packet Filter）是Linux中最炙手可热的技术之一，用于在Linux内核中执行安全、可编程的字节码，可应用于网络管控、系统跟踪、安全监控、性能分析等领域，具有高灵活性、可扩展性和强安全性。

* 高灵活性：开发人员可按需编写自定义的eBPF程序，从而实现各种功能。
* 可扩展性：支持动态加载和卸载不同的eBPF程序，而无需重新编译内核。
* 强安全性：在内核中执行eBPF的字节码之前，会对eBPF的字节码进行严格的验证和限制，既能实现eBPF的灵活编程能力，也能保障系统的稳定性和安全性。

▶KProbes

Kprobes是Linux内核中的一种动态跟踪机制。

* 允许在内核函数的入口和出口插入探针，以便观察函数的调用和返回情况。
* 允许在内核的关键代码路径上插入探针，以便捕获和分析各种内核事件的信息，如函数调用次数、参数值、返回值等。
* 可驱动eBPF程序，实现内核级别的事件跟踪和分析。

▶eBPF Maps

eBPF Maps是一种键值对数据结构，由键（key）和值（value）组成。

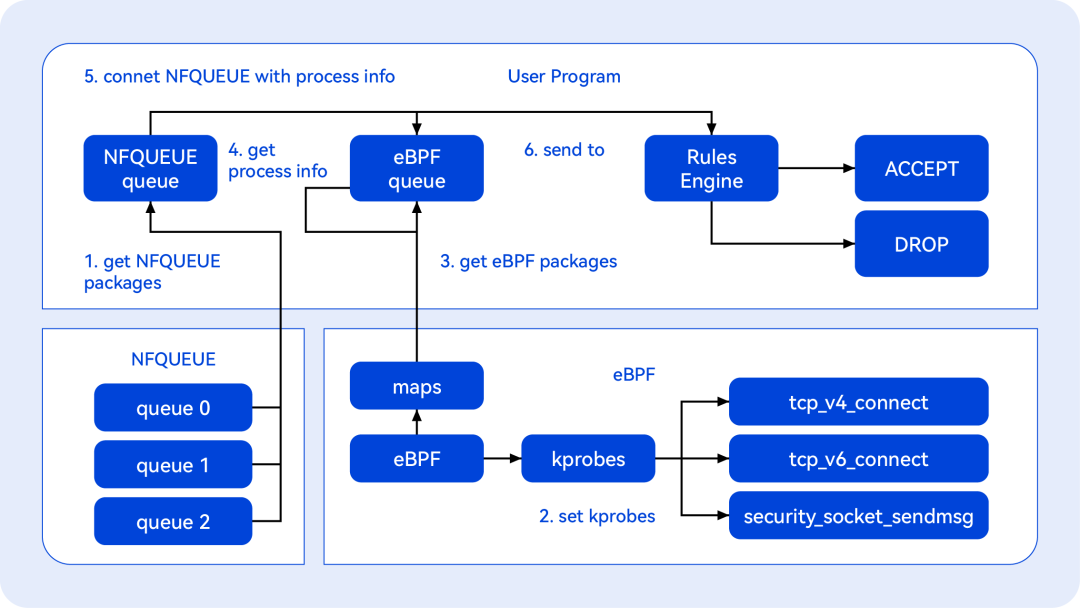
* 支持自定义键和值的类型，并在eBPF程序中进行读取、写入和更新操作。
* 支持在用户空间和内核空间之间安全地传输数据。

▶NFQUEUE

NFQUEUE通过使用Netfilter框架中的hook机制，将选定的网络数据包从内核空间传递到用户空间进行处理。

                                 统信有固：与时俱进

六个关键步骤



1、使用iptables配置NFQUEUE规则，将系统中的网络数据包转发到NFQUEUE队列。

2、通过eBPF程序在内核网络协议栈相关函数的入口和出口插入Kprobes探针。

3、当有网络流量产生时，系统会截获其中的每个网络数据包并将其送入eBPF程序。eBPF程序获取进程ID（PID）后，会将PID与网络数据包进行绑定，最后通过eBPF Maps将绑定好PID的网络数据包送入用户空间。

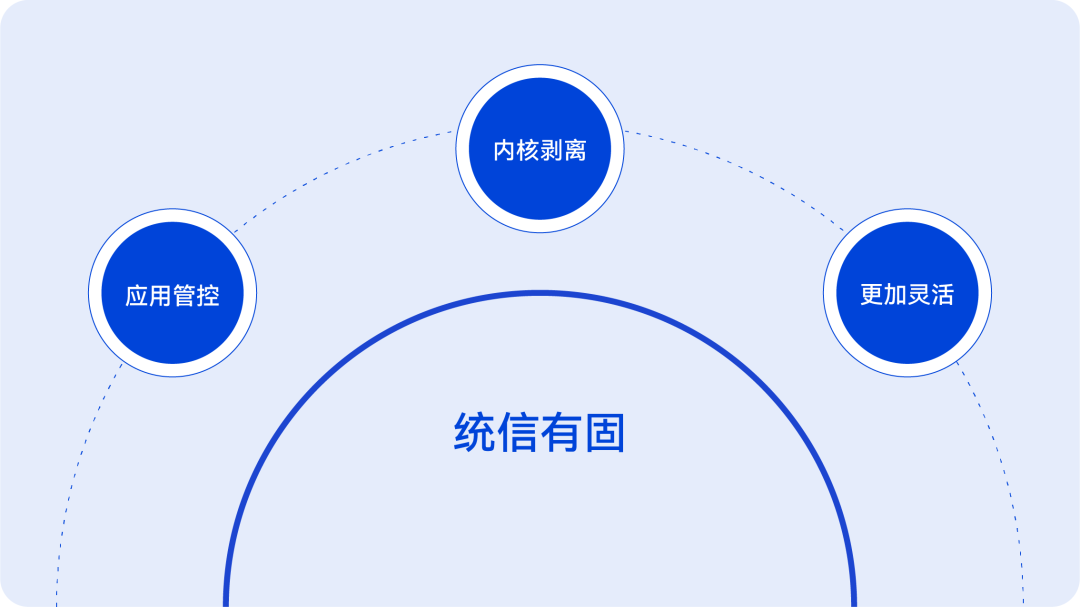
4、在用户空间中，通过PID可以获取进程的相关信息，例如启动时间、文件路径、进程状态等，然后收集并保存这些信息后供后续使用。

5、通过IP地址、端口号、协议类型等信息，用户态程序将NFQUEUE队列中的网络数据包与eBPF模块捕获的网络数据包进行关联，从而获取NFQUEUE队列中每个网络数据包对应的进程信息。

6、将NFQUEUE队列中的网络数据包送入规则引擎，通过对比已配置好的流量规则，可以判断是否接受或丢弃这些网络数据包。

三大突出优点

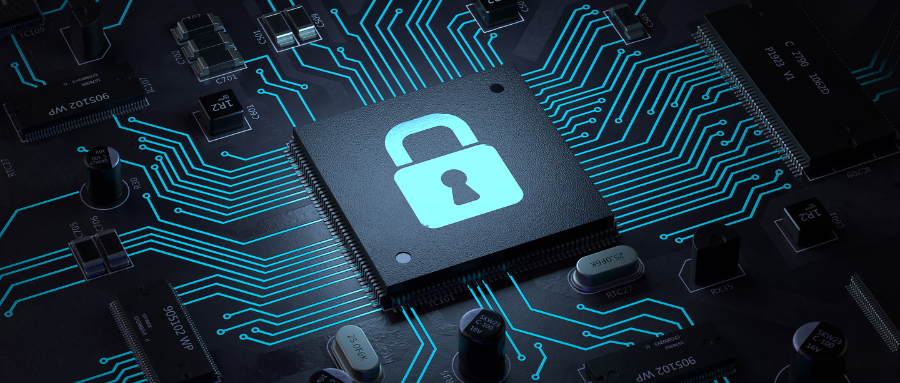
传统的Linux网络管控方案，如iptables、firewalld等，都只能工作在网络层和传输层，而「统信有固」的网络管控方案可以将网络管控扩展到应用层。



「统信有固」的网络管控方案采用内核剥离技术，其独特之处在于无需修改内核源码，这一创新不仅大幅提升了系统的安全性，还为适配不同的Linux系统带来了更大的便利性。

同时，「统信有固」的规则配置、网络管控方式更加灵活，可以针对单个应用进行规则配置，也可以实现定制化的管控方式。

统信软件一直坚持提供极致的安全防护，不仅拥有最严苛的流程管理、最极致的设计理念，更重要的是拥有最硬核的安全技术。本次推出的「统信有固」新方案，是对统信UOS服务器版全栈系统安全防护体系的进一步完善和升级。



**统信UOS服务器版**汲取国内外主流社区技术栈优势，深入技术底层结合国内外设计标准与规范以及各类用户业务应用需求，积极开展技术创新，全面支持国内外主流CPU架构和处理器厂商，在各种应用环境中，满足**强安全、高稳定、高性能、易维护以及泛兼容**等要求，是构建信息化设施环境的基础软件产品：

◈强安全：

* 等保四级GB/T 20272-2019认证
* 商密二级GM/T 0028认证
* 全栈生态链支持国密
* 国际知名安全社区OpenSCAP官方首批支持的中国操作系统
* 21天推送一次补丁更新，每周进行漏洞修复推送

◈高稳定

* 稳定版 Linux 4.19&5.10双内核
* 热补丁升级机制
* LTP 7\*24小时测试用例通过率超98%
* 长时高负荷运行，卸荷后60秒内实现系统及各应用流畅运行

◈高性能

* 内存拷贝页技术，拷贝性能提升超70%，满并发优化提升10%
* 多种自研性能优化成果：文件读写性能提升4%、调度延迟减少10%、多并发锁竞争场景性能提升5%……
* 相比同类产品，UnixBench等测试全面领先

◈易维护

* 提供自研统信有易服务器迁移软件
* 提供自研统信有幄自动化运维工具
* 提供面向场景的AI系统调优能力

◈泛兼容

* 历史版本兼容性>98%，提供平滑升级方案
* 组件模块化设计，为用户最大限度解决底层依赖问题
* 全面通过整机适配兼容性测试（多种不同型号的整机）



**统信软件服务器操作系统与云计算产线总经理孟杰**表示，我们正在加快脚步，让统信UOS进一步满足不同领域、不同场景的安全应用要求，打造坚实可信的安全根基，为AI等新技术形态下的国家信息安全战略保驾护航。我们相信，「统信有固」即将推出的全新应用层网络管控方案，不仅可以保障系统安全，还能大大提升整个网络的可管理性，进而为客户带来更优质的网络体验。

©统信软件技术有限公司。访问者可将本网站提供的内容或服务用于个人学习、研究或欣赏，以及其他非商业性或非盈利性用途，但同时应遵守著作权法及其他相关法律的规定，不得侵犯本网站及相关权利人的合法权利。除此以外，将本网站任何内容或服务进行转载，须备注：**该文档出自【faq.uniontech.com】统信软件知识分享平台**。否则统信软件将追究相关版权责任。