亿阳网警 BOCO．SFW-3000 防火墙

技术白皮书

1. 概述

亿阳网警 BOCO．SFW－3000 防火墙是包含防火墙，VPN，IDS，内容安全，流量控制，高可用性，安全管理等七个特性，为用户提供全面的网络安全保障的网络安全设备。

防火墙的作用是防止内部的信息系统遭受外部的攻击。它划定了一个边界，使经认证的局域网用户和管理员以及独立工作站和单机用户可以安全访问不可信的外部网络或接受这些外部网络的访问。它使边界中的所有成员都可以防止未授权系统的侵入、数据被修改和删除、拒绝服务和窃取资源或服务等攻击。防火墙能够使边界中的用户使用安全连接，数字处理、信息的传输和存储都受到保护。

防火墙技术经过了十几年的不断完善，目前正处在技术的发展变化时期：在系统结构上朝着采用专用平台与专用协议栈、易于拓展方向发展；在功能上朝着功能完备、面向用户应用，进行细粒度的分析与过滤方向发展；在管理上朝着面向管理者，人性化方面发展；在性能上，朝着高吞吐率、高并发联接、低丢报率，能够保证网络报文高速、完整的传输方面发展。由亿阳信通设计并生产的亿阳网警系列防火墙本着用户需求第一的准则，采用了面向技术发展方向的设计思想，在全新的体系结构中融入了性能优异的专用算法，实现了防火墙管理的强安全性、高性能、高稳定性、利于管理，并具有易于扩展等特点。亿阳网警系列防火墙代表了防火墙技术的发展方向，将在相当一段时间内作为保护用户网络边界安全的主力军大量地应用于用户的各种业务网络和办公网络。

亿阳网警 BOCO. SFW－3000 防火墙系列产品是基于状态检测的新一代高性能、高安全性产品。它稳定、可靠、抗攻击能力强、功能丰富、易于管理，适用于政府、企业、军队、公安、电子商务网站、金融、银行、税务、证券、教育等部门网络。

亿阳网警 BOCO．SFW－3000 系列防火墙具有高速全状态包过滤、应用透明代理、MAC 地址绑定、OTP/RADIUS 用户认证、SNAT/DNAT 双向地址转换功能、负载均衡功能，还提供了入侵检测、流量控制、虚拟专用网、日志服务、安全审计与报警等安全功能，系统配置管理基于控制台及 WEB 界面，灵活方便。支持全透明网络接入、VLAN 环境、双机热备等，可为用户网络提供理想的安全

解决方案。

亿阳网警 BOCO．SFW－3000 防火墙系统符合 GB/T18336-2001、GB/T18019-1999 和 GB/T18020-1999 等国家标准，已经通过公安部计算机信息系统安全产品质量监督检验中心的检测。被权威评测机构“赛迪评测”评为精品防火墙产品。

2. 产品系列

防火墙系列包括：

亿阳网警 BOCO．SFW－3000E－－企业级百兆防火墙

亿阳网警 BOCO．SFW－3000P－－电信级百兆防火墙

亿阳网警 BOCO．SFW－3000G－－千兆防火墙

亿阳网警防火墙日志服务器－－系列防火墙的通用审计日志集中统一处理平台

3. 系统特点

完全硬件实现

亿阳网警 BOCO．SFW－3000 防火墙系统完全固化在 FLASH ROM 中，属硬件防火墙，具有专用性强、稳定性高、速度快等特点。

专用操作平台

亿阳网警 BOCO．SFW－3000 防火墙系统采用自主研发的专用安全操作系统作为整个系统的基础平台，由于专用的安全操作系统没有后门、漏洞以及多余的服务，极大地提高了防火墙系统的自身的安全性。

丰富的协议支持

亿阳网警 BOCO.SFW-3000 系列防火墙支持多种数据链路层、网络层、应用层协议，可以适应各种用户网络环境。

强安全性

亿阳网警 BOCO．SFW－3000 防火墙提供了多种保护网络的安全措施，如果配置得当，可以保证用户网络的安全。

抗攻击能力强

亿阳网警 BOCO．SFW－3000 防火墙自身带有抗攻击模块，可以抵御已知的 13 大类包括几百种攻击行为。

灵活的接入方式

亿阳网警 BOCO．SFW－3000 防火墙提供多种接入模型，可以以路由方式接入，也可以以桥方式透明接入；可以有多个 IP 地址，可以只有一个 IP 地址，也可以没有 IP 地址，满足用户的各种网络环境的接入需求。

实现完全透明

亿阳网警 BOCO．SFW－3000 防火墙系统做到了真正的透明，即无论使用任何功能，对正常的用户来说防火墙系统都可以做到是不可感知的。很显然这样做有两个好处：

1、防火墙系统的安装和卸载都不会影响网络的任何一部分，管理人员可以平滑地安装和卸下亿阳网警 BOCO．SFW－3000 防火墙系统。

2、减少了用户的操作。一般情况下，用户为了使用代理服务器，要在客户端的应用程序（如浏览器、FTP 程序）上设置代理的 IP 地址和端口，而且还要有一个前提，就是客户端应用程序必须支持代理（有很多种客户端应用程序是不支持代理的，如 TELNET 程序），使用亿阳网警 BOCO．SFW－3000 防火墙系统用户不必做任何设置，就可以使用代理服务，极大地方便了网络用户。

实时的响应能力

亿阳网警 BOCO．SFW－3000 防火墙在防火墙日志服务器的配合下，可以做到对紧急事件（如黑客的入侵）的及时响应，并可以通过 E-mail 等手段向管理人员报警。

方便的操作使用

亿阳网警 BOCO．SFW－3000 防火墙的安装和卸载都十分的简便，并且不会影响网络的其它设备。

人性化的对象化管理

对象化管理封装了防火墙的底层控制对象，使防火墙策略保持稳定。亿阳网警 BOCO．SFW－3000 防火墙对防火墙管理控制对象进行对象化管理，对象层的引入使防火墙策略对易变的底层控制对象保持稳定。

简单的配置管理

无论利用哪一种管理方式，用户都可以发现亿阳网警 BOCO．SFW－3000 防火墙的配置非常之简单。

优异性能的性能指标

亿阳网警 BOCO．SFW－3000 防火墙系统基于高速的硬件平台和优良的操作系统平台，保证了整个系统运转和网络传输的高速安全。

超强的扩充能力

亿阳网警 BOCO．SFW－3000 防火墙系统的硬件和软件都是采用模块化设计，用户在购买基本系统之后，可以根据需要增加相应的软硬件模块，扩充系统能力。

实时的日志集中统一管理

为用户提供了实时的日志集中统一管理平台，具有链路层事件、网络层事件、应用层事件、入侵事件、操作事件等多种日志信息，日志实时地发往日志服务器，日志服务器可以进行日志的查询、统计、整理、事后分析、对紧急事件的报警等功能

完整的失败恢复机制

防火墙采用双机热备份机制和配置双备份机制，能在多种灾难条件发生的情况下，保证防火墙安全正常地工作。

4. 功能特点描述

4.1. 专用系统软件平台 BOS

专用系统软件平台 BOS 包含防火墙，VPN，IDS，内容安全，流量控制，高可用性，安全管理等七个特性，为用户提供全面的网络安全保障，具有操作系统安全性更高，性能更加优化的特点。

4.2. 全状态高速包过滤功能

亿阳网警 BOCO.SFW-3000 防火墙采用了全状态检测的包过滤技术。利用状态检测技术可以对报文进行深度分析和处理，相对于静态包过滤具有更高的安全性和更加优异的性能，即使在增加上万条安全策略的情况下，也不会降低防火墙的网络性能。亿阳网警 BOCO.SFW-3000 防火墙的包过滤功能可控制项包括：

源 IP 地址

目的 IP 地址

协议类型（ICMP、TCP、UDP）

源 TCP/UDP 端口

目的 TCP/UDP 端口

TCP 报文标志

IP 分组选项域

ICMP 报文类型域和代码域

包通信的日期和时间（包括起始时间、终止时间、星期、日）

可以对报文或联接进行日志记录和统计。

4.3. 地址转换 SNAT 和 DNAT

地址转换可以起到隐藏内部网络结构和解决 IP 地址不足的问题。亿阳网警 BOCO.SFW-3000 防火墙支持双向地址转换功能（SNAT 和 DNAT）：

- SNAT 在 IP 层上通过对源地址的转换提供 IP 地址复用，解决 IP 地址不

足的问题，对外隐藏内部的网络地址；

- DNAT 在 IP 层上通过对目的地址的转换可以达到外部网络对内部网中服务器的访问，实现解决 IP 地址不足的和对外隐藏内部网的作用。

亿阳网警 BOCO.SFW-3000 防火墙支持一对一的地址转换、一对多的地址转换、多对一的地址转换和多对多的地址转换。

4.4. VPN 及客户端

支持 IPsec 协议：Authentication Header（AH）协议、Encapsulating Security Payload（ESP）协议和 IKE 密钥交换协议。

在支持 3DES（数据加密标准）基础上，支持 AES（高级加密标准），使之加密强度更高，加密速度更快。

支持两种工作模式：传输模式和隧道模式。

支持 IKE 密钥自动协商和密钥手工配置两种模式。

支持 NAT 穿越。

VPN 客户端提供预共享密钥方式，L2TP+IPSEC 方式，预共享密钥+BOCO 扩展认证，证书方式，书+BOCO 扩展认证等 5 种用户认证方式，保证用户方便，灵活，安全的接入方式，为用户提供接入安全保障。

4.5. 异常检测及入侵检测功能

内嵌对异常协议数据包的检测与阻拦。

对于各种扫描和攻击防火墙或防火墙所保护网络的行为，按事先设置的规则库，进行比较匹配，并执行相应的报警和日志记录。它作为防火墙的基本功能的合理补充，帮助系统对付网络攻击、及时发觉系统漏洞，扩展系统管理员的安全管理能力。

可以检测出 33 大类，千余种黑客的攻击行为，主要的类别包括：

- 扫描探测；
- DOS 和 DDOS 攻击
- WEB 攻击；
- 木马攻击；
- Land Attack；

- Ip Source Routing；
- Ip Spoofing；
- 缓冲区溢出攻击；
- 蠕虫攻击；
- FTP 或 TELNET 非法用户登录；

由于采用了先进的报文预处理和模式匹配技术，亿阳网警 BOCO.SFW-3000 防火墙内嵌的入侵检测功能具有低误报率、低漏报率、高性能等特点。用户可以自主设置检测的敏感度，同时还具有与第三方入侵检测产品联动的能力。

4.6.内容过滤功能

在透明代理基础上实现了 URL 过滤和文本内容过滤功能，屏蔽不良的、非法的网站，对 WEB 内容的进行细粒度的精确过滤和控制，防止所有内部网用户浏览邪教、色情等不良中外网站及网页。

该功能适合于中小学校、大专院校、政府、企业和某些专业应用场合使用。可彻底杜绝对用户访问不该访问网站的忧虑，净化了网络环境、节省了带宽。亿阳网警 BOCO.SFW-3000 防火墙内容过滤功能支持如下协议：

HTTP1.1 协议
HTTP1.0 协议
支持对如下内容的过滤：
URL 过滤
站点过滤
文件扩展名过滤
搜索引擎缓存过滤
过滤 google 等搜索引擎的缓存内容
智能加权过滤
MIME 文件类型过滤
关键字过滤
ACTIVEX,JAVS script 过滤

管理员可以通过内容过滤监控用户的 WWW 浏览链接。其中的智能加权过滤技术可以极大的提高内容过滤的准确性，是亿阳网警 BOCO.SFW-3000 防火墙

的一个先进技术特色。除此之外，亿阳自主的内容过滤功能还具有如下特点：

快速 URL 过滤：URL 库的规则为 10 万条时，每秒种可以过滤 40 万个 URL；
内部网不用更改任何设置，网络数据库的防范及过滤完全由工作核心完成；
只有具备管理员身份才可登录到工作核心进行防范设置更改；
可对一切用户违规的行为留下日志记录；

4.7. 网络带宽管理功能

虽然近年来网络带宽几乎每十二个月就翻一番，但带宽的发展永远达不到用户对带宽的要求，为了保证用户关键业务拥有足够的带宽，亿阳网警 BOCO.SFW-3000 防火墙提供了完整的带宽管理方案，包括

根据策略进行流量控制；

提供精密的带宽共享及流量优先级别控制；

为个别流量及总体流量提供服务级别保证；

基于防火墙对象控制机制，可以根据主机 IP 或子网段，服务类型（ftp、http 等）、时间分配带宽

亿阳网警 BOCO.SFW-3000 防火墙采用分层树算法作流分类算法，在保证带宽控制的准确性的同时，不会带来性能的降低。

4.8. 双机热备及负载均衡功能

支持服务器负载平衡。可以将一个外部 IP 地址映射为多个内部 IP 地址，对每次 TCP 连接请求动态使用其中一个内部地址，达到负载均衡的目的
支持高可用性。亿阳网警 BOCO. SFW-3000 防火墙实现了主从式双机热备功能，配置友好方便，对防火墙失效状态判断准确全面可靠，从机接管切换快，使用户网络防火墙节点单点失效的风险最低。
支持防火墙集群。

4.9. 防火墙接入模式

网络接入支持路由，NAT，透明，桥接等接入模式。

路由模式（路由，NAT）下防火墙除了进行网络边界的访问控制同时具有路

由功能，可以节省用户的投资。

透明模式(透明，桥)下无论是安装防火墙还是卸载防火墙，都不必改变网络的拓扑结构，不需修改网络设备的参数与设置，在用户端亦不必做任何修改和设置就可以实现基于 IP 协议的各种信息的传输，此种模式下用户可以选择是否让防火墙具有 IP 地址。

支持 pppoe 拨号，DHCP 服务器，VPN/客户端等功能，适用于各种应用模式。

4.10. 透明代理

代理的功能是对来自局域网内的用户的会话请求进行转发。从安全角度讲，这样做有以下几个用处：

1、完全阻断了网络的传输通道。

2、可以进行访问控制。

3、隐藏了内部网络结构，因为最终请求是由防火墙发出的外面的，外部主机并不知道与哪个用户通信。

4、解决 IP 地址紧缺的问题。使用代理服务器只需防火墙有一个公网的 IP 地址。

亿阳网警 BOCO.SFW-300 防火墙的代理服务器具有如下优点：

- 支持多种 TCP 上层协议
- 完全的透明性，对防火墙以外的任何设备以及主机无需做任何修改
- 与包过滤及 NAT 统一的策略规则配置，便于用户统一管理。

4.11. 用户认证与授权功能

用户认证主要是针对通过防火墙的数据进行认证。

适合于院校、政府、企业和某些专业应用场合使用。可彻底杜绝没有经过认证用户对计算机资源的访问。认证方式支持：

- 本地用户认证
- OTP(一次性口令)；
- RADIUS 认证；

客户端支持透明认证和非透明认证两种方式：

- 透明认证：透明地在用户要通过防火墙请求服务时认证的功能(支持

TELNET 和 WWW 服务透明)，认证后用户权限在管理员配置的时间内有效

- 非透明认证：用户主动向防火墙要求对其进行认证的功能(支持 TELNET 和 WWW 方式主动认证)，认证后用户权限在管理员配置的时间内有效。

4.12. 安全审计功能

由于黑客行为的发展呈多样化趋势，绝对的安全是根本不存在的。在这种现实情况下，一个优秀的日志系统的作用显得十分突出，如果审计信息完备有效，用户就可以根据历史事件找到黑客的蛛丝马迹，进而对破坏者进行法律上的惩罚，以及通过对原有的安全策略进行调整来提高网络的安全性，封堵漏洞。

亿阳网警 3000 防火墙实现了审计信息的分布式管理，审计信息实时地由防火墙发往日志服务器。日志服务器是审计信息的集中统一管理中心，运行于标准配置 PC 服务器的亿阳网警日志服务器系统可以集中处理来自数百台亿阳网警防火墙设备的审计信息。审计的种类包括：

- 对链路层非法协议包的审计；
- 包过滤模块支持对网络 IP 层和传输层（TCP/UDP/ICMP）审计功能
- 入侵检测模块的审计和报警功能；
- 对应用层代理的审计；
- 对系统管理层的审计，包括对审计模块操作的记录；对用户认证与授权的记录；系统关启记录等；

日志信息仅在防火墙缓存一定数量，定时的发往日志服务器，用户也可以主动的从防火墙端读取最新日志。

4.13. 实时报警功能

黑客的入侵是一个需要一定时间的过程，根据 PDRR 原理（保护、检测、响应和恢复）降低检测时间和响应恢复时间是阻断攻击的前提，因此亿阳网警 BOCO.SFW-3000 防火墙实现了实时报警功能，给管理员以最快的响应时间，报警方式支持：

EMAIL

控制台

用户自定义

4.14. MAC 地址绑定功能

地址绑定的主要作用是防止非法用户盗用合法用户的 IP 地址，由于每块网卡的 MAC 地址都是固定的，经过地址绑定后，IP 地址就与计算机或用户（若每台计算机的用户固定）的对应关系就固定了。也就是说，只有特定的主机才能使用特定的 IP 地址，这就可以保证 IP 地址不被盗用。

亿阳网警 BOCO.SFW-3000 防火墙支持手动和自动两种地址绑定方式。

4.15. VLAN 支持功能

随着结构的愈加复杂，网络对 VLAN（虚拟局域网）协议的支持已经必不可少，利用 VLAN 技术，可以将物理网络划分为多个逻辑的局域网，以达到网络层次和结构更加清晰、减少网络被大面积攻击的可能。亿阳网警 BOCO.SFW-3000 防火墙支持最主要的两种 VLAN 协议，包括：

- ISL
- 802.1q

4.16. 开放的联动接口

BOSV2.2.1 同时提供开放的联动接口，支持与第三方安全产品(IDS，防病毒网关)的联动，最大限度地保护用户的安全投资。

4.17. 版本升级和规则导入导出

防火墙功能模块和安全服务升级支持两种方式：

- 手工升级：将升级软件包直接送到管理员手中；

- 在线升级：管理员通过安全信道将升级软件包取到本地。

支持防火墙规则的导入导出功能，方便了用户规则的备份及恢复。

4.18. 状态信息显示功能

用户可以利用此功能来远程监视防火墙的运行状态，亿阳网警 BOCO.SFW-3000 防火墙提供给用户如下信息的显示：

- CPU 使用率：
- MEM 使用率：
- 并发连接数目及当前连接状态信息
- 双机热备的状态信息
- 支持 SNMP 状态查询功能

4.19. 防御攻击

防火墙内置抗 synflood, udpflood, icmpflood, land attack, ping sweep, teardrop, smurf 等攻击保护，且用户可配置参数。

5. 系统安全性

5.1. 安全性分析

亿阳网警 BOCO.SFW-3000 防火墙完备的安全机制可以保障内网和其自身的安全：

- 多层过滤和控制机制

亿阳网警 BOCO.SFW-3000 防火墙基于核心 IP 层的全状态检查和应用层的透明代理检查，可以对 IP 地址、网络服务、网络协议、信息内容等进行有效控制和过滤，可以避免对内网的非法访问和有害信息入侵；

- 入侵检测和抗攻击机制

有效检测和抵御了黑客的对内网及防火墙的入侵和破坏；

- 日志审计及实时报警机制

及时发现潜在的危险和正在遭受的入侵行为，有效提高内网和防火墙的安全，并可作为事后追查的依据，做到“亡羊补牢”；

- 安全管理配置机制

防火墙管理员的分级授权管理，身份认证与授权，管理信道上信息的加密传输，专用安全平台等机制可以确保防火墙远程配置管理的安全；

5.2.系统抗攻击试验

目前，常见的黑客攻击手段主要有以下几类：利用协议漏洞进行的攻击，拒绝服务攻击，代理服务，IP 欺骗，网络端口扫描，系统信息搜集，缓冲区溢出等。

在对亿阳网警 BOCO.SFW-3000 防火墙进行的抗攻击性实验中，使用了北京北方计算中心研制的网络安全性分析系统 Internet Security Explorer 3.0 和 Linux 下的 Nessus 等软件对亿阳网警 BOCO.SFW-3000 防火墙进行了扫描和攻击实验。实验进行的项目及得到的测试结果如下表所示：

测试项目	测试结果	测试项目	测试结果
邮件服务	通过	网管协议	通过
强力攻击	通过	WINDOWSNT 服务	通过
守护进程	通过	NT 用户组/网络配置	通过
远程过程调用	通过	网络共享/DOCM	通过
网络文件系统	通过	NT 安全配置与审计	通过
拒绝服务	通过	WINDOWSNT 安全区	通过
NETBIOS 及其它	通过	文件传输协议	通过
WINDOWS 用户及其它	通过	网络端口扫描	通过
WINDOWS NT 注册表	通过	NT 信息搜集	通过

WINDOWS NT 口令	通过	系统信息搜集	通过
代理/域名服务系统	通过	特洛伊和后门程序检测	通过
WWW,HTTP,CGI	通过	FIREWALL	通过
IP 欺骗	通过	浏览器	通过

6. 配置管理

6.1. 安全管理

在一个网络系统中，能否实现管理的安全是实现网络整体安全的关键所在。亿阳网警 BOCO.SFW-3000 防火墙采用了最为先进的管理理念和多种安全管理技术，为实现管理的人性化和安全性提供了全面的可行方案。

1、采用加密技术实现信息传输的安全

亿阳网警 BOCO.SFW-3000 防火墙利用集加密、认证和信息完整性校验为一体的 SSL 安全套接层协议进行管理信息的传输，可以有效地保证防火墙的管理信息不被非法者截取以及防止黑客进行重播攻击。

2、多种认证方式实现对用户的鉴别

亿阳网警 BOCO.SFW-3000 防火墙采用了多种用户鉴别机制，包括本地用户认证、OTP 一次性口令认证和 RADIUS 认证。用户可以根据实际情况采用不同的认证方式。其中 RADIUS 认证方式适合用户数量大，服务器较多的网络。

3、采用分级管理的方式实现管理权限的划分

亿阳网警 BOCO.SFW-3000 防火墙将管理员按权限分为系统管理员、安全管理员和审计管理员，实行管理权限的分级具有如下优点：

1）有效的防止防火墙管理人员的越权操作

2）对于技术水平不足的管理员，赋予较低的权限，可以防止由于误操作造成的安全漏洞。

3）实行权利分摊，减少具体某个管理员的工作量。

6.2. 管理的分类

基于串口终端的本地管理

基于 WEB 的远程管理

基于 SSH 的远程管理

7. 日志服务器

亿阳网警 BOCO.SFW-3000 防火墙日志服务系统针对当前客户对防火墙日志管理的不同需求，提供了有效的日志服务解决方案。日志服务器系统遵循模块化设计的思想，提供了后台服务模块和用户 GUI 工具模块，很好的解决了防火墙日志的接收、日志扫描、告警、查询等功能。其主要特点有：

- 合理的结构化设计：日志服务系统除驻留在防火墙主机的日志代理，做到功能的独立。减轻了防火墙处理日志的负担，同时增强了日志的处理功能。日志服务系统统一负责日志的存储、查询、分析、报警等功能。
- 安全的传输机制：防火墙日志的发送采用 TCP 连接，而且有完善的确认和校验机制，避免了日志的丢失。
- 集中的日志管理：日志服务器可以集中接收管理多台防火墙的日志,强大的日志备份及导入功能。
- 方便友好的日志查询：对日志进行组合查询，并提供对查询结果的编辑和打印。
- 实时日志扫描：对包过滤日志准确有效的分析，快速检测出可能的网络攻击。
- 控制台和邮件告警机制：及时的将入侵和系统告警显示或利用邮件发送给管理员。
- 面向对象的流量统计功能：可对用户定义的网络对象提供流量查询及图表显示打印功能。

8. 性能指标

8.1. 系统物理参数

8.1.1 百兆系列物理参数

输入电压：220V

有效功率：90W

网络接口：10/100Base TX 3 个（可扩充同类型网络接口）

配置用 Console 口：RS232。

正常工作温度：-5~50ºC

8.1.2 千兆兆系列物理参数

输入电压：220V

有效功率：200W

网络接口：百兆以太网接口 2 个、千兆多模光线接口 2 个（可扩充千兆多模光线接口、千兆单模光线接口、千兆铜缆接口以及百兆以太网接口）

配置用 Console 口：RS232。

正常工作温度：-5~50ºC

8.2. 系统性能指标

8.2.1 百兆系列性能指标

3000-E:

64 字节帧长的条件下为线速的 50%（100 兆）。256 以上字节帧长的条件下均达到或接近线速的 100%。

时延：28~40μs

丢包率：0。

最大会话连接数：50 万

3000-P:

所有帧长的条件下均达到线速。

时延：30~50μs

丢包率：0。

最大会话连接数：32 万

8.2.1 千兆系列性能指标

吞吐率：

64 字节帧长的条件下为线速的 22%（220 兆）。512 以上字节帧长的条件下均达到或接近线速的 100%。

时延：15~30μs

丢包率：0。

最大会话连接数：100 万（可扩充到 200 万以上）