浪潮网络

TQ2000防火墙版本说明书

(TSOSV206R0600B20240219)

目 录

1. 序

1.1 目的

下一代防火墙系统 TSOS V206R0600B20240219 的版本特性进行总体说明。

1.2 适用范围

本文档的适用范围为下一代防火墙系统 TSOS V206R0600B20240219 的版本。

1.3 术语表

无

1.4 参考资料

无

2. 概述

2.1 发布说明

下一代防火墙系统 TSOS V206R0600B20240219 版本，对比上一个版本是大规模功能补强的重要的技术版本。改进点主要有以下几个方面：

1. 标杆特性添加。包括 vsys 虚拟防火墙、ssl 加密流量审计、报表等。
2. 一些顽固市场问题的攻克解决。比如数据库文件损坏等。
3. 标志性新硬件的引入。比如 E2000Q 等

产品软件版本信息： TSOS V206R0600B20240219

Bootloader 版本信息：V4.2

3. 功能特性

3.1 功能特性

功能	子功能	功能描述	备注
网络	SSLVPN	SSLVPN 支持国密（不含国密加密卡）	优化
	SSLVPN 客户端	SSLVPN 客户端支持 Windows、linux、MAC OS 等操作系统，并可支持麒麟、统信等国产化操作系统	

SSL 加密流量检测		支持客户端模式和服务器模式两种工作模式	新增
		支持对 HTTPS、POP3S、SMTPS、IMAPS 等协议的加密流量检测。	
		独立的 SSL 流量检测策略。策略包含对入接口（安全域）、源地址、目的地址的控制。	
		SSL 解密后的流量，支持 AV、IPS、口令防护、web 防护、恶意文件检测、应用控制、web 控制等应用层业务。	
		支持域名白名单功能。并有预定义白名单库。	
		支持 IP 地址白名单功能。	
		客户端支持根 CA 推送，支持网站证书自动签发。	
虚拟防火墙		支持以 VRF 和 VSYS 为基础的虚拟化技术。可以单独配置虚拟系统（虚拟防火墙）或虚拟路由器（仅虚拟路由隔离）。根据设备物理内存大小，可配置的虚拟路由器和虚拟防火墙数量上限不同，最大为 256。	新增
		虚拟系统创建时，支持对新建、并发、吞吐、安全策略数量，NAT 规则数量、对象数量等资源做限制。	
		虚拟系统支持创建内部虚拟接口，实现虚拟防火墙和根系统之间流量互通	
		虚拟系统和虚拟路由器支持接口隔离：包括物理接口、vlan、透明桥、链路聚合、GRE 等。虚拟系统更支持安全域的隔离	
		虚拟系统和虚拟路由器支持路由隔离：包括直连路由、静态路由、动态路由、以及会话保持等	
		虚拟防火墙支持 NAT 规则以及 NAT 地址池的隔离。	
		虚拟防火墙支持地址对象、服务对象、与应用对象、用户对象、时间对象的隔离	
		虚拟防火墙支持防护策略的隔离；并支持病毒防护、入侵防护业务的配置	
		虚拟防火墙支持下列统计以及曲线的隔离展示：整机流量、新建并发连接、CPU 内存的统计曲线；支持接口以及接口应用统计 top10 曲线；支持威胁统计曲线以及威胁 top10 统计；会话统计及会话流量统计。	
		虚拟防火墙支持下列日志类型的隔离：系统日志、NAT 日志、防火墙日志、病毒防护日志、入侵防护日志、流日志	
		虚拟防火墙支持系统管理员的隔离。	
安全防护	恶意文件检测	基于恶意文件库的恶意文件检测功能	新增
		支持 HTTP、FTP、IMAP、SMTP、POP3 等协议的文件还原并检测。	
		支持恶意文件库的自动升级和离线导入	
		支持手动添加或删除恶意文件特征（目前仅支持命令行）	
	口令防护	口令防护支持 SSH 协议	优化

系统	报表	支持对如下信息进行报表展示： 1. 网络及安全风险概况（概览）。包含流量概览，应用和用户概览、威胁概览 2. 网络流量详情。包含整机流量曲线、新建连接曲线、并发流量曲线、接口流量 top10 3. 应用统计及风险详情。包括应用流量排行、应用分流流量排行、应用详情。 4. URL 活动及风险详情。包括 URL 访问排行、URL 访问分类排行、URL 详情等。 5. 用户统计详情。包括用户流量排行、用户并发连接排行、以及 TOP 用户的应用排行。 6. 网络风险威胁详情。包括威胁级别统计曲线、威胁主机排行、威胁类型分布、以及各 TOP 攻击的子类排名。 7. 威胁说明（对各种网络威胁的文字说明）	新增
		支持自定义和预定义模板。选择关注的内容生成报表	
		可基于选定模板生成报表任务。支持立即生成或周期计划，周期计划可知 1 天/7 天/30 天。	
		支持全局参数配置，包括统计引擎是否开启、当前报表文件占用空间大小、自定义封面图片导入等	
		支持对当前设备已存储的报表进行汇总展示。支持以生成时间对报表进行过滤检索，支持对选定报表进行导出和清除操作	
	软件虚拟化	支持生成带 mgt 口（带外管理接口）和不带 mgt 口（带外管理接口）的两种镜像	优化
		支持添加或删除虚拟接口，不影响原有接口命名以及序列号校验。	

4. 技术积累及问题

4.1 技术积累

1. 支持了标准 VRF；数据平面业务模块的 VSYS 隔离的经验；
2. 支持了 7 层协议栈，以及 SSL 解密/卸载的流程；积累了浏览器证书推送和网站证书签发的经验
3. 支持了飞腾 E2000Q 的 SOC 方案；积累了裕太交换芯片驱动的开发经验（底端国产化解决方案的初步尝试）

4.2 解决的问题

1. 针对设备异常掉电后引发的日志错误、文件系统损坏等问题作了统一的梳理：
   1） 设备异常掉电并再次启动后，对硬盘进行自检。
   2） 设备每次启动后对日志文件进行数据库完整性检查，删除损坏的日志文件。
   3） 对日志量大的业务模块进行限速。NAT、安全策略等。
2. 解决了一系列的 ike v2 的 bug，ike v2 的可用性大大提升
3. 使用 cpu_limit 对 IOT 扫描任务进行限制，避免控制平面 cpu 占用过高。将来也可以用于其他任务。
4. 解决了由于 SSH 终端启用 ext-channel 造成的 vtysh 异常的 bug。

5. 版本注意事项

5.1 版本发布配套组件版本号

Php：8.2.9；SSH：9.4

5.2 平台限制

支持发布的硬件平台。

5.3 组网中注意事项或应用限制

无。