浪潮网络

TQ2000防火墙版本说明书

(TSOSV206R0500B20230324)

目 录

1. 序

1.1 目的

本文对 TQ2000 系统 TSOS V206R0500 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 TQ2000 系统 TSOS V206R0500 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

防火墙 TQ2000 TSOSV206R0500 版本，在 TSOSV206R0411 版本的基础防火墙业务功能之上，进行了一系列功能和易用性的补强。此版本的特性更新分为以下几类：

一. 重大竞争性功能特性添加。例如资产防护。

二. 常规安全功能进一步补强。例如黑白名单、域名黑名单、口令防破解、漏扫联动、威胁情报等。

三. 针对农行 IPS 项目的功能补齐。例如 IPS 抓包、自定义事件集升级、XFF 字段上报等。

四. 重大易用性优化。例如审计日志、策略预编译、域名地址对象等。

从上述内容可以看出，5.0 版本是 TSOS 系统一次全方位的补强版本。对增强产品竞争力，以及作为后续技术版本的基础，都是非常有利的。

2.2 版本信息

产品软件版本信息： TSOSV206R0500B20230324

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
防火墙	安全策略	策略预编译开启后自动更新，且修改策略相关的地址对象、接口安全域等，预编译会自动更新	功能优化
		策略配置超时事件扩大	功能优化
资产防护	资产防护及展示	针对用户网段的防护列表，配置主动及被动探测、以及针对资产不同属性的告警。	新增功能
		资产列表展示，针对资产的信息展示、审批、搜索、导入等功能	
	资产扫描及指纹管理	支持对资产的扫描，可动态获取资产的 MAC 地址、厂商、类别、操作系统、端口等信息	
		包含内置预定义指纹库，支持预定义指纹库升级。支持自定义指纹库，并支持根据当前资产扫描结果一键生成自定义指纹	
	资产安全	支持资产黑名单、资产 IP-MAC 绑定。并支持根据资产扫描结果一键生成黑名单以及 IP-MAC 绑定	
	交换机联动	支持通过 snmp 获取三层交换机内网资产的 MAC 地址列表	
	行为学习	可自动学习资产的连接关系列表、并根据连接关系一键生成安全策略，或执行一键抓包	
安全防护	黑名单	新增 IP 地址范围的配置	功能
		支持黑名单分组，支持基于分组的一键启停	
		支持起始生效事件配置，并支持失效后自动删除，支持一键删除已失效表项	
		支持引用 ISP 地址库	
	IP 地址白名单	支持基于单 ip、ip 地址范围、ip 网段、区域地址、ISP 地址库的 IP 白名单，可跳过后续安全策略、防护策略等	新增功能
	口令防暴力破解	支持对口令暴力破解的自动识别，支持对检测强度的配置，以及动作的配置	新增功能

	IPS	针对 IPS 事件集的抓包功能。可选择扩展抓包（触发事件的会话所有报文）和单包抓包（触发事件的当前报文）。抓到的报文可以通过列表展示并通过事件名称及时间过滤，也可以在入侵防御日志页面直接检索	功能优化
		自定义事件集更新，事件集展示增加是否为新增事件	功能优化
		IPS 事件 XFF 字段展示。在 IPS 事件日志 content 中加入 XFF 字段解析。	功能优化
	威胁情报	支持离线库匹配。离线库支持自动升级和手动升级。离线库匹配不到还可进行云查。	功能优化
		威胁情报对域名的识别支持针对 DNS 报文	功能优化
	域名黑名单	支持对指定域名（精确或模糊）dns 的检测和阻断。	新增功能
安全联动	漏扫联动	支持和启明星辰漏扫产品联动，获取终端列表。	新增功能
		可在防火墙管理页面针对终端下发漏扫任务，支持在威胁主机展示页面直接下发漏扫任务。	
对象	地址对象	域名地址对象支持被动探测，支持模糊匹配，支持老化。	功能优化
网络	网络调试	页面支持 ping v6	功能优化
系统	配置	配置文件支持周期性配置到本地，并支持恢复或导出	新增功能
		命令行超时时间可以在页面配置并保存	新增功能
		Web 页面可以修改密码要求长度	功能优化
	系统快照	ARM 平台支持系统快照（无硬盘不支持）	功能优化
	时间	NTP 支持备份服务器	功能优化
		NTP 支持认证	
	日志	审计日志重构，每一条业务配置可以体现为添加、删除、修改。且每一条参数配置项的改变都可以体现在审计日志中。	功能优化
		支持 8 个 syslog 服务器	功能优化
	运维	一键导出设备异常信息	新增功能
	告警	日志硬盘占用达到阈值，产生告警日志	功能优化

4. 版本注意事项

4.1 版本发布配套组件版本号

Php：7.4.32；SSH：8.9

4.2 平台限制

支持发布的硬件平台。

4.3 组网中注意事项或应用限制

无。