永达电子

安全可信接入风险控制网关

产品概述

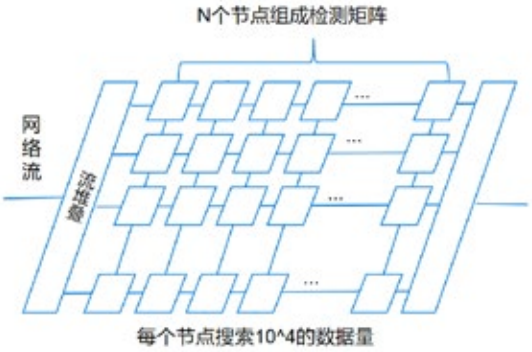
安全可信接入风险控制网关以大数据为底座、海量数据分析为依托构建安全可信网络环境，同时在网络边界上实现业务行为的可信度量和双向访问控制，实现抵御各种未知攻击的能力。

在算力支撑上基于表征的存算一体模型，实现基于内容的联想记忆与分类识别；在算法上通过构建组织、防护、检测、响应、恢复（即 OPDRR）的框架，构筑可信防线，实现系统与网络的高安全等级保护。

产品功能

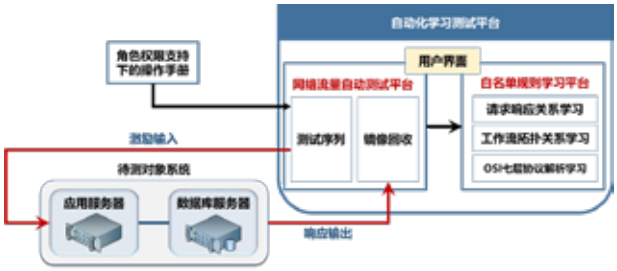
01 资源组织-O（组织）

主要聚焦于各安全部件组织调度编排，并由多个检测单元构成检测矩阵，对主要资产和网络流量进行报文特征、请求响应关系、频域特征等多重检测。



02 布防图勾勒-P（防护）

关注人机环境等全网要素，将资产分布集、功能权限集、操作行为集、漏洞库、病毒库、攻击库、以及安全目标、安全要求、安全策略、安全模型纳入保护规划中。对企业虚拟资产进行标识、配置、归类形成资产保护对象。



02.1－可信行为模型生成

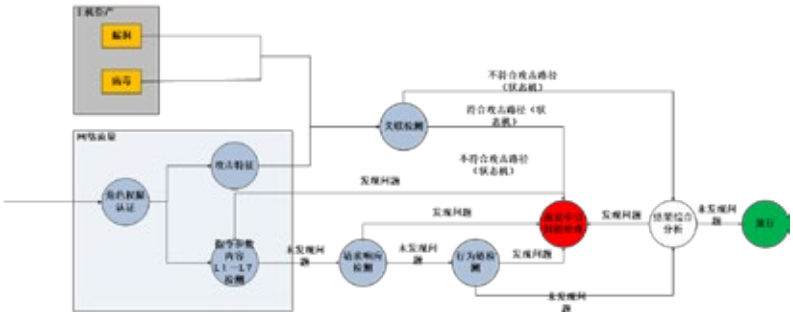
包括业务应用建模和网络流量建模两部分，业务应用基于操作手册完成，网络流量基于自动化测试平台，大数据训练学习的方法自动完成建模。

02.2－网络攻击模型生成

从攻击者的角度出发，建模网络攻击模型，并分析为了达到攻击的目的所必备的攻击条件、攻击步骤及攻击步骤之间的关联关系，并有针对的展开一系列的攻击行为。

03 矩阵式全流量检测引擎—D（检测）

提供了矩阵式全流量检测引擎，从主要资产和网络流量上全面检测，包括攻击特征、请求响应、行为、行为链等多重检测。



03.1－面向攻击层面的降风险安全防护

- **入侵防御**

在蠕虫、后门、木马、间谍软件、Web攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计等防御手段。

- **病毒防护**

拥有海量病毒特征库，配合先进的防病毒引擎，能够精准识别并清除流行木马和顽固病毒。

- **异常流量过滤**

异常包攻击防御检测单元，可以检测各项偏离预期的网络行为。依据RFC 标准规范制作通信协议异常检测模块，可以阻止不符合标准通信协议规范的数据包。支持网络流量异常检测，可以准确地检测网络流量的异常情形。

03.2－面向应用层面的安全可信防护

根据应用层面的操作学习的业务健康工作流，对网络报文在OSI七层上映射特征进行检查过滤、对操作的主客体标记进行权限检查、对请求与响应的对应关系进行检查、对报文间的时序关系进行检查，实现业务行为的结构化保护。

- **七层检测**

基于 OSI 七层协议的体系架构，对物理层、链路层、网络层、传输层、会话层、表示层、应用层各层进行过滤检测。

- **状态机检测**

支持基于业务状态机的检测，当前发生的状态与预期状态机不一致时，状态机检测异常告警。

- **双向检测**

对服务器发起的请求以及服务器的回复包进行双向内容检测，使得敏感数据信息不被外发，实现攻击事件发生前的预防以及攻击事件发生后的检测及补救。

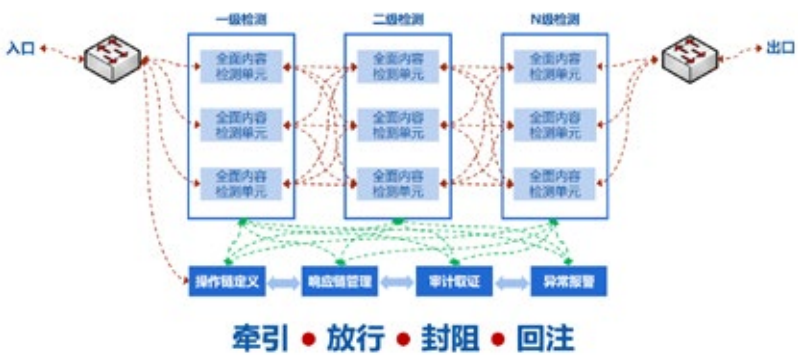
- **标记检测**

对主体，客体设置安全标记，支持安全标记检查，确保访问主体的可信。所有主体及其所控制的客体（如进程，文件，设备、字段等）实施强制访问控制。

04 流量牵引与封阻—R（响应）

对一个已知攻击事件发生之后，安全可信接入风险控制网关通过流量牵引、放行、封阻、回注进行响应，转移、减少、化解安全威胁。

安全可信接入风险控制网关具备以下基本功能：



04.1－蜜罐引流

流量牵引就是将攻击流量和正常流量进行分离，由封阻子系统来专门抵抗未知攻击，保证正常流量尽可能的不受到攻击的干扰。当发现异常时，能自动将异常流引流到蜜罐，跟踪记录整个过程，便于追踪攻击路径，发现业务漏洞。

04.2－阻断

对非法操作进行阻断。

04.3－告警信息

流量牵引与封阻能对非法访问等提供报警功能，报警信息应至少包含以下信息：恶意 IP 地址、恶意操作链、事件发生的日期和时间。

04.4－定制响应

系统应允许管理员对被检测网段中指定的目的主机定制不同的响应方式。

04.5－告警方式

告警应采取屏幕实时提示、E-mail 告警、Syslog 告警等一种或几种方式。

04.6－其他设备联动

系统应具有与其他网络设备或网络安全部件（如漏洞扫描、交换机）按照设定的策略进行联动的能力。

04.7－策略路由

04.8－流量会话管理

04.9－流量统计

能够根据用户 / 用户组、IP 地址、应用类型，配置最大带宽、保障带宽的参数，划分带宽优先级；能够支持基于时间段的带宽策略配置。

04.10－连接数控制

能够限制单 IP 的最大会话数，防止大量非法连接产生时，影响网络性能。

04.11－NAT

支持双向 NAT:SNAT 和 DNAT；支持动态 SNAT 技术，实现“多对多”的 SNAT。

04.12－信息泄露防护

具备对流出的信息流进行检测，防止敏感信息泄露。

05 容错恢复—R（恢复）

安全可信接入风险控制网关可感知每个检测单元的状态，当单个检测单元失效时，通过重载、重配、重构交换网络实现功能恢复。

产品参数

安全功能		
组织(O)功能	全交换管理	能力识别、自动编排、并行检测、故障转移
防护（P）功能	资产识别	
	拓扑关系识别	
	未知协议训练与识别	
	业务特征自学习	
	业务状态机配置	
检测（D）功能	网络层访问控制	包过滤、IP/MAC绑定、状态检测、DDOS攻击防护
	风险降级防护	应用协议访问控制、应用内容访问控制 、用户管控、信息泄漏检测、入侵检测与防护、WEB攻击防护、病毒检测、流量统计、流量控制
	安全可信防护	业务行为特征检测、业务状态机检测
响应（R）功能	安全审计	记录事件类型、日志内容、日志管理
	报警	
	联动防御	
恢复（R）功能	应急恢复	快速应急响应与恢复
网络服务功能	NAT、路由控制、应用代理	
安全云化管理	管理安全、管理方式、管理能力、管理接口独立、安全支撑系统、异常处理机制、事件管理、高可靠性、升级	
性能要求	应用层吞吐量、网络层吞吐量、延迟、最大新建连接数、最大并发连接数	

产品性能	
吞吐量（bps）	20G
每秒连接（K）	600
并发连接（M）	10
威胁防护	10G
基线匹配时延	≤1 秒

⋆ 规划中产品规格，具体当前可配置信息以详细产品手册为准。

产品亮点

01

无干扰可信模型

一种基于系统操作无干扰的完整性度量模型，该模型借鉴信息流的无干扰理论，通过分析进程操作的完整性及进程间完整性的传递，从动态的角度对系统的运行完整性进行度量。

02

基于自动化测试框架的基线学习

通过自动化操作测试与服务响应模拟测试，建立用户应用操作工作流基于操作者、操作指令、服务响应链、操作负荷数据等的配置项，通过应用模拟运行测试建立在网络报文流量行为的表征基线和事件时空序列基线。

03

网络行为的可信度量

通过自动化测试框架的学习的表征基线使用工作流模型形成形式化基线的专家系统，由检测矩阵对当前的网络流基于形式化基线进行可信度量，实现基于网络可信行为的访问控制。

客户案例

- 中华人民共和国工业和信息化部
- 中华人民共和国应急管理部
- 中国国家铁路集团有限公司
- 北京经纬信息技术有限公司
- 成都市应急管理局
- 通号通信信息集团有限公司
- 中共中央统一战线工作部
- 中华人民共和国科学技术部
- 北京市东城区人民政府
- 中国十八个铁路局集团有限公司

⋆本产品符合以下国家标准：

- GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》
- GA/T 1177-2014 《信息安全技术 第二代防火墙安全技术要求》（增强级）

深圳市永达电子信息股份有限公司
Shenzhen Y&D Electronics Information Co, Ltd.

★ 国家级高新技术企业 ★ 国家信息安全服务二级资质企业
★ ITSS二级资质企业 ★ 涉密信息系统集成甲级资质企业

地址：深圳市南山区科技北一路17号摩比天线大厦5楼
电话：0755-26727588 传真：0755-26727593
邮箱：sales@s-ec.com
官网：http://www.s-ec.com

售后热线 400-884-0006