

# 安全资源容器



SR-Container-A

## 产品概述

云融统一安全防御系统 (USD) 是集**安全服务链**、**安全资源容器**、**安全管理平台**为一体的网络安全整体解决方案。其中**安全资源容器(SR-Container)**内嵌**防火墙**、**WAF**、**入侵检测和防御**、**上网行为管理**、**数据库审计**、**数据库防火墙**等原生态安全服务，并且可集成任意支持虚拟化部署的第三方安全服务。根据用户的不同安全等级与需求，可以自由选配安全服务、灵活调度安全资源，解决安全扩容难点，从而打造一个灵活、高效、全面的网安融合解决方案。

## 产品特点

### 高性能的网络和安全处理能力

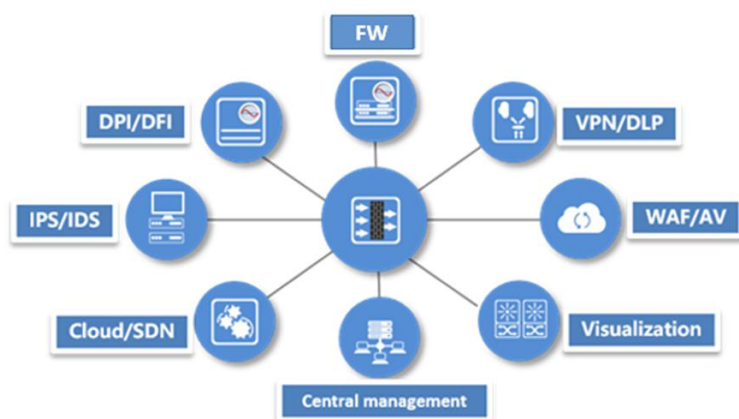
SRC 采用业界先进的多核并行架构和 DPDK 零拷贝技术，在硬件抽象层上运行自主知识产权的安全 OS，高效的资源调度算法和流量分发机制，提高网络流量处理性能。

SRC 内置一体化的报文处理引擎，通过对数据包一次解析，按业务层次由对应模块处理，可以节省不同模块间重启解析数据包所消耗的资源，提高安全业务处理性能。

### 全面的安全防护能力

SRC 产品内嵌自主可控的虚拟安全管理平台系统，集防火墙、负载均衡、入侵防御、数据

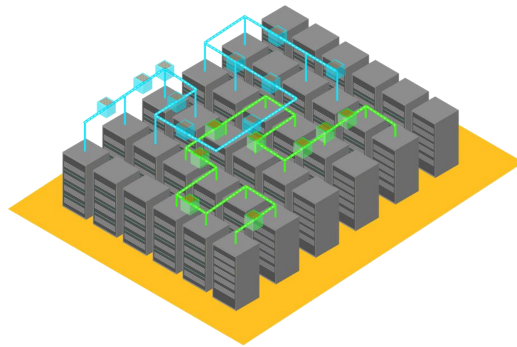
库审计与防护、上网行为控制等功能于一体,针对不同的用户需求调用对应的安全防护组合,按需引流。



- 具备精细化应用管控,可为用户提供多维的应用风险分析和筛选,以及灵活的安全控制,包括策略阻止、会话限制、应用引流和智能流量管理等。同时,还具备入侵防御、病毒过滤、攻击防护、链路与服务器负载均衡、NAT 等功能,满足客户对安全访问,攻击防护以及应用识别和控制等需求。
- 具备 VPN 接入能力,可与物理防火墙或虚拟化防火墙建立安全加密隧道,确保数据的远程安全传输。可为网络管理员提供远程后台管理的安全访问通道,也可为混合云的组建提供安全、可靠,性价比高的安全互联通道。
- 具备 HA 组网能力,满足配置和会话同步的要求,从而实现高可靠的冗余部署,保障用户业务的不间断连续运营。

## 保护东西向流量安全

在网络中网络威胁会将横贯东西向的方式在 VM 之间移动、传播,直接影响到租户的业务与数据安全。我们基于零信任原则,在 VM 间部署 SRC,对横向网络的应用业务系统、工作站与跳板机等流量进行控制,减少威胁暴露面积。



## 数据库审计与防护

支持以旁路或串行方式部署侦听的工作模式，能对 Oracle、MS-SQL Server、DB2、Sybase、MySQL、Informix、CACHE、teradata、神通（原 OSCAR）、达梦、人大金仓（kingbase）等业界主流数据库进行深度解析与审计分析，可以帮助用户提升数据库运行监控的透明度，降低人工审计成本，真正实现数据库全业务运行可视化、日常操作可监控、危险操作可控制、所有行为可审计、安全事件可追溯。

## 多台虚拟化安全性能扩容

云融 SRC 使用软件定义网络，支持多台安全设备虚拟化，便于以后更大规模的扩容。

云融 SRC 可虚拟多台安全设备，配合安全服务链使用，可最大化的利用其性能及后期升级扩展。

云融 SRC 虚拟出的安全设备都可以与业务一一对应，相互完全隔离。

## 集中统一的可视化管理

用户可对设备资源进行统一管理，进行设备零配置上线，统一的策略管理，业务变更自学习，攻击事件监控、攻击事件分析、报表分析等。可以极大的降低了网络的更换难度，简化了运维成本。

云融 SRC 可视化的监控页面可提供系统监控、用户流量、设备流量、会话监控、事件告警，威胁分布供维护人员及时了解网络的健康和安全状态。

### 监控统计

- 支持系统资源监控、接口状态、实时流量、会话数、用户流量、应用流量的监控统计
- 支持威胁分布与威胁统计功能
- 支持自定义时间刷新监控页面功能
- 支持对云内资源流量与应用的多维统计监控
- 支持报表发送与导出功能
- 支持告警发送功能，包含 CPU 告警、内存告警、会话告警、流量告警、ipsec-vpn 连接断开告警

### 防火墙

- 基于应用识别的深度访问控制
- 基于应用/角色/时间的安全策略
- 丰富的路由特性
- 强大的 NAT 及 ALG

### 行为管理

- 根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、vlan 等信息划分管道
- 支持两层四级管道嵌套的带宽限制和保证
- 支持最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证
- 基于时间和优先级的差分服务，支持带宽均分策略
- 对剩余带宽根据优先级进行弹性分配
- 基于角色、时间、优先级、页面类型等条件的 web 网页访问控制

## 攻击防护

- 支持 ARP 攻击防护
- 支持多种异常包的攻击防护，支持 IPv6 异常包攻击防护
- 支持 SYN Flood 、 DNS Flood 等多种 Dos/DDos 攻击防护
- 支持扫描攻击防护
- 支持攻击黑名单

## 入侵防御

- 基于状态、精准的高性能攻击检测和防御
- 实时攻击源阻断、IP 屏蔽、攻击事件记录
- 支持针对 HTTP、SMTP、IMAP、POP3、VOIP 等几十种协议和应用的攻击检测和防御
- 支持缓冲溢出、SQL 注入和跨站脚本攻击的检测和防护
- 支持专业的 Web server 防护功能，含 CC 攻击防护和外链防护等
- 支持自定义入侵防御特征
- 提供预定义防御配置模版
- 提供几千种特征的攻击检测和防御，特征库支持网络实时更新

## 数据库审计与防护

- 基于深度协议分析技术，实现对网络中的数据库资产进行自动添加并归类分组，整个过程无需人工添加；同时实现 SQL 数据审计。
- 能对 SQL 语句的执行结果（成功或失败）、执行时长、返回行数、绑定变量值进行深度解析，帮助客户有效的提升审计内容的精确性。
- 提供了黑白名单、自定义告警规则、审计例外、内置漏洞特征库等安全配置策略，帮助客户及时发现威胁，并告警。

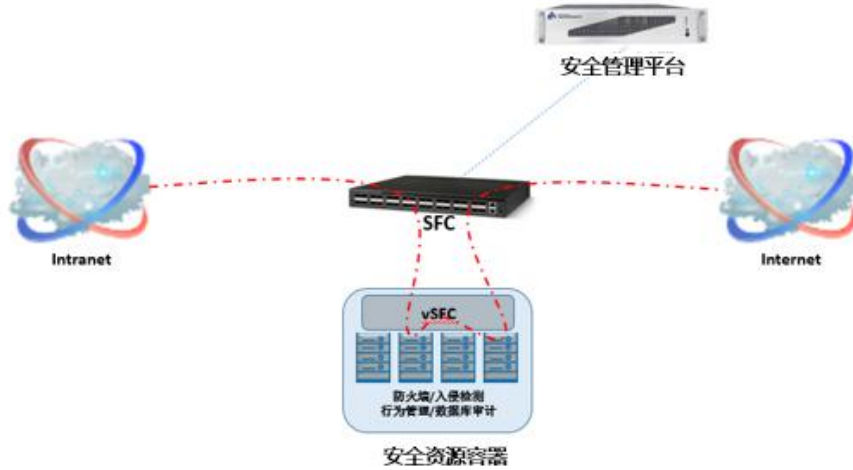
- 能对数据库的在线连接的会话进行实时监控, 帮助客户更好的了解数据库并发会话数的状态。
- 提供了邮件、短信、ftp、syslog、snmp 等告警方式, 可以自主选择告警方式。

## **链路负载均衡**

- 基于 7 元组、域名、接口、接口组的链路负载均衡策略
- 基于直连网段和特定网段的负载均衡排除
- 负载均衡接口支持 PPPOE、DHCP、聚合链路等三层接口
- 支持接口探测
- 支持基于源地址 hash 的链路负载均衡
- 支持基于优先级的链路负载均衡

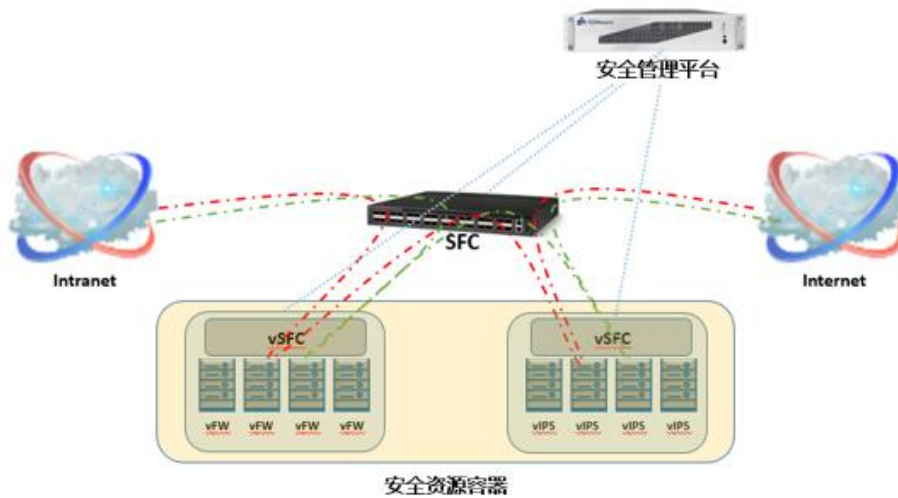
## 产品功能

### 多种安全设备统一部署



## USD 统一安全防御系统

### 多台虚拟化安全性能扩容



## USD 扩容解决方案

### 苏州云融信息技术有限公司

地址：中国科大苏州研究院内（苏州工业园区仁爱路 166 号）

电话：400-998-7338

官网：www.sdnware.com

Copyright ©2020 苏州云融信息技术有限公司保留一切权利

免责声明：虽然苏州云融试图在本资料中提供准确的信息，但不保证资料的内容不含有技术性误差或印刷性错误，为此苏州云融对资料中的不准确不承担任何责任。苏州云融保留在没有通知或提示的情况下对本资料的内容进行修改的权利。