迷宫网络攻击捕获系统

江苏君立华域信息安全技术股份有限公司

产品概述 | Product Overview

君立华域研发的迷宫网络攻击捕获系统，是一款用于保护业务、捕获攻击、发现系统漏洞的网络安全主动防御蜜罐产品。“蜜罐”基于传统“蜜网”技术、却又解决了传统“蜜网”技术部署复杂、技术单一、无动态结构变化、诱捕手段不全、识别不准确等问题，是将传统信息安全手段从被动防御变为主动防御的革命性产品，是重要信息系统防护的重要壁垒。

功能特性 | Features

蜜罐部署

“迷宫”内置丰富的蜜罐资源，包含系统服务蜜罐、web 服务蜜罐、中间件蜜罐、数据库蜜罐等常见的业务类型的蜜罐，还可以根据用户的需求和真实业务定制定制蜜罐。多类型的蜜罐进行组合，可最大限度实现对真实业务网络的仿真，迷惑并诱捕攻击者。

高安全性

由于蜜罐类产品的特殊性质，当蜜罐被攻破、利用成为跳板机时，会造成更严重的损失。所以蜜罐产品的自身安全性更为重要。君立华域“迷宫”网络攻击捕获系统有着更为严格的安全特性：

- 蜜罐攻破自毁：“迷宫”系统中部署的蜜罐被攻破后，会在用户自定义的时间内自毁，避免成为攻击者的跳板机，并且会在自毁前备份蜜罐数据，以供取证溯源；
- 网络安全组：可在蜜罐所在节点配置网络安全策略，设置网络流量可以单向流通，防止流量从蜜罐向外访问，导致内网其他系统被渗透；
- 通信加密：“迷宫”管理节点和蜜罐节点之间的流量传输经过加密，可避免被攻击者截获后分析破解；
- 白名单：“迷宫”可设置白名单，仅运行白名单内的 IP 地址访问“迷宫”的管理节点。

探针蜜罐

“迷宫”提供探针功能，可部署在真实网络环境的业务系统、主机、办公电脑中，对网络中的扫描、探测、攻击等行为进行监控，将数据反馈于主节点用于系统捕获分析。

迷宫网络攻击捕获系统

阻断联动

“迷宫”可与防火墙设备进行联动，将捕获的攻击者特征同步给防火墙，由防火墙自动生成安全防护策略，阻断相应的攻击流量。防火墙可部署在网络中任何位置，整个阻断联动过程无需人工干预。

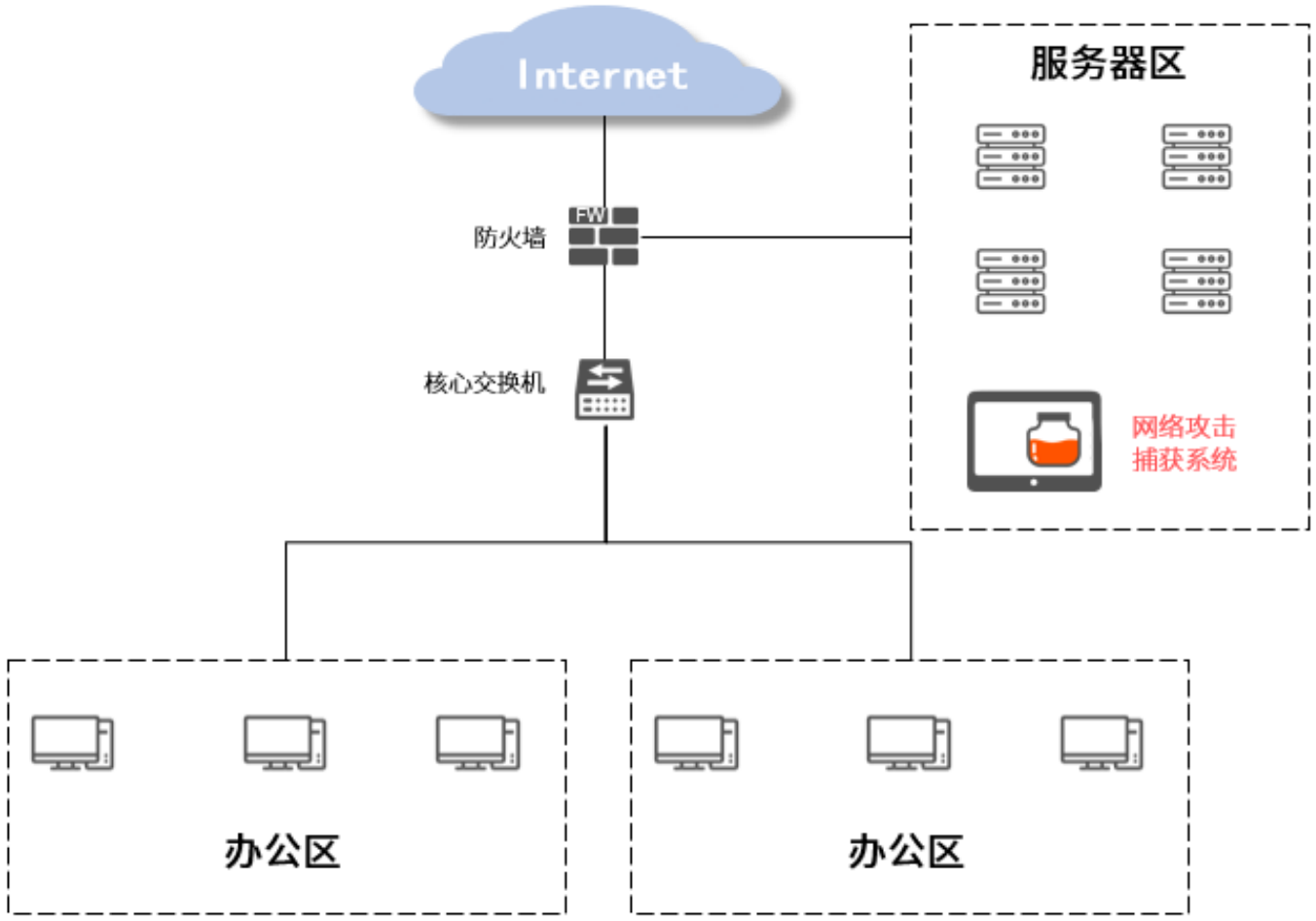
黑客溯源

“迷宫”可捕获的攻击者攻击特征并溯源攻击者的信息，包括源 ip、源物理地址、设备指纹、攻击数量、威胁指数、真人概率、攻击类型、攻击服务、攻击常用工具、常用攻击命令等。可记录攻击者上传文件、修改文件、删除文件的行为轨迹。管理员可下载攻击者上传的文件进行分析。

攻击录像

“迷宫”可对攻击者的攻击行为进行录屏，通过录像对攻击者的攻击行为、攻击工具、攻击习惯等特征进行分析。

典型应用 | Typical scene



技术参数 | Technical Parameter

产品型号	君立华域迷宫网络攻击捕获系统
蜜罐环境	支持运行系统服务蜜罐、数据库服务蜜罐、Web 服务蜜罐、中间件服务蜜罐等常用服务的蜜罐环境，包括 ssh、Samba、MySQL、MongoDB、tomcat、gitlab、splunk、struts2、crm、weblogic、redis 等常用服务，受到攻击后可以查询攻击者源 IP、源物理地址、攻击时间、攻击次数、遭受攻击的环境、行为轨迹等数据；
	用户可自己上传蜜罐镜像，并定义该镜像的日志路径、漏洞类型、系统版本、交互等级、危险等级、支持的服务、端口号、CVE 号等属性；
	可根据企业需求定制仿真企业型蜜罐，高度仿真企业实际业务系统，以达到迷惑黑客且保护企业真实业务系统的目的；
	支持部署低交互蜜罐或高交互蜜罐，低交互蜜罐通过脚本模拟真实系统，安全性更高；高交互蜜罐使用真实系统诱捕攻击者，仿真度更高；
	支持关联多个蜜罐环境组成特定业务场景，可通过业务场景模板一键部署多个蜜罐；
	提供 Agent 探针，将攻击用户真实业务系统的流量引流到蜜罐中；
	支持 NAT 方式和 VLAN 方式设置蜜罐 IP 地址；
蜜罐安全	当黑客成功入侵系统后，在可控时间内会自动关闭该蜜罐环境，确保系统安全；在关闭蜜罐环境的同时，将该蜜罐进行备份，用于人工取证；
	支持添加安全组策略，可自定义添加蜜罐流量出入站规则，限制蜜罐流量外发，防止蜜罐成为跳板机；
	支持设置访问控制策略，限制特点 IP 地址访问蜜罐管理界面；
入侵检测	可根据文件的变化、异常进程检测黑客的入侵行为，并形成日志记录；
	可感知端口探测行为，并形成日志记录；
	能够识别出常见扫描器的种类，比如 Nmap、awvs，并形成日志记录；
	根据 Payload 去检测黑客的入侵行为和威胁等级，并形成日志记录；
	支持对每个蜜罐单独定义添加检测规则，包含规则内容、攻击方式、危险等级、触发类型等；
阻断联动	可与网络层设备联动，当蜜罐被攻击后，立即将攻击者网络层特征同步给联动设备，联动设备立即对攻击进行阻断；
	可设置阻断联动周期，当设置的周期时间到达后，阻断策略自动删除；
	可手工设置阻断策略，包括阻断的 IP 地址和阻断周期，拦截外部攻击；
溯源取证	支持对黑客的操作进行进行视频实时记录，支持视频实时播放和回放，用于取证；
	支持对黑客的攻击行为轨迹按时间线进行记录；
	实时记录蜜罐节点访问流量，并支持 PCAP 格式下载；
	支持对黑客攻击进行溯源，包括：源 ip、源物理地址、攻击数量、威胁指数、真人概率、攻击类型、攻击服务、攻击常用工具、常用攻击命令、设备指纹、攻击拓扑图；