天翼云产品培训材料

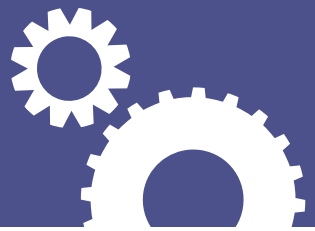
云下一代防火墙

产品与生态部

2022-7-19

/03 天翼云云下一代防火墙可以用在哪?

- 典型场景是什么?
- 标杆项目有哪个?

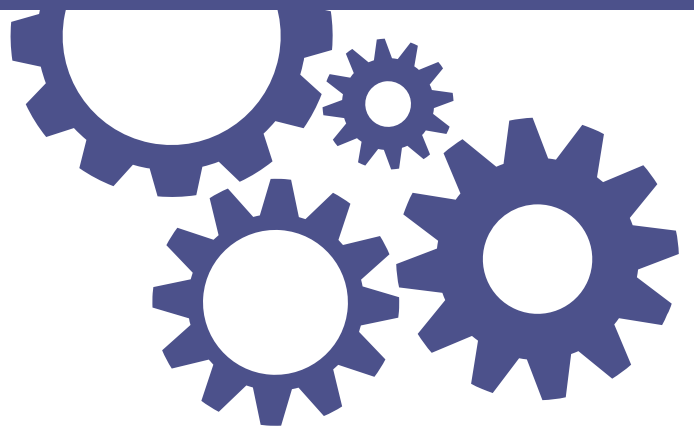


/01 为什么要用云下一代防火墙?

- 市场趋势是什么?
- 客户痛点是什么?

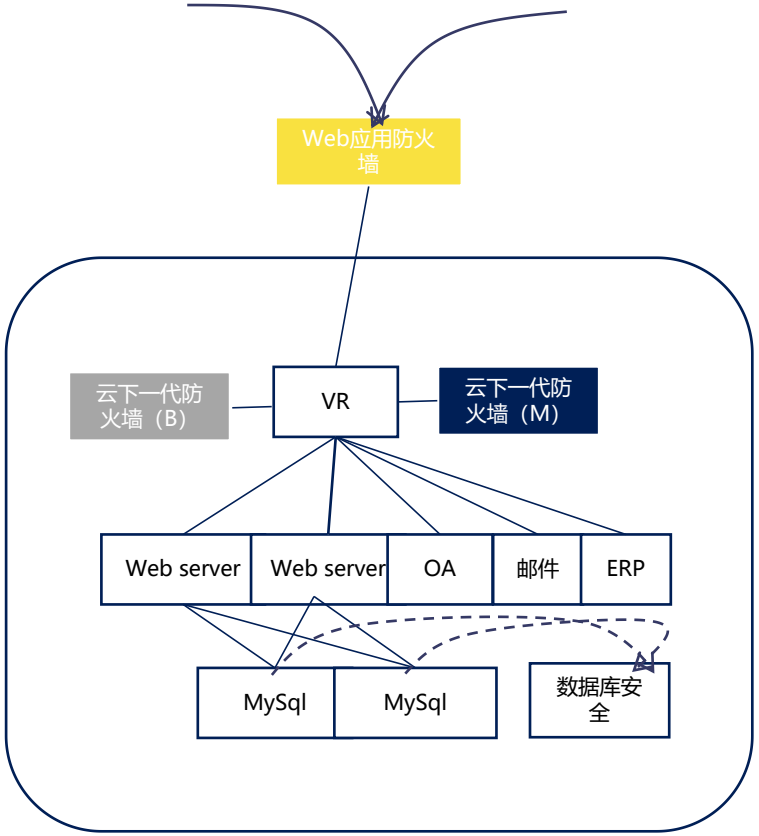
/02 天翼云云下一代防火墙是什么?

- 产品有什么能力?
- 和业界比能力如何?



产品典型使用场景：云下一代防火墙对网站&应用系统防护

- 场景说明：
  - 有网站&应用系统的客户
  - DDos攻击&暴力破解&勒索病毒/挖矿木马等攻击防护
- 基本状况：
  - 客户有网站及其它OA、邮件等业务上云，需要保证VPC具有入侵防御和病毒过滤等功能；
  - Web服务器云主机需要通过一些安全手段来实现恶意的暴力破解、DDos攻击及被勒索病毒感染/挖矿木马利用的防护，保证服务器资源利用，增强业务安全性；
- 防护效果：
  - 通过云下一代防火墙实现访问流量经过病毒过滤和入侵防御的模块检测之后再达到具体的业务云主机；
  - 网络安全产品特征匹配，网络层限制并发/新建数；
- 实际案例：
  - 中国电力建设股份有限公司
  - 国寿(三亚)健康投资有限公司
  - 济宁市卫生和计划生育委员会



额外增值销售场景：小微企业可以单独购买云上防火墙对本地物理网络防护

- 需求：部分中小企业用户为了减少投资，将物理网络里面的安全设备迁移到云上进行安全防护。
- 场景：客户物理网络通过云专线与上云业务打通。此时将弹性IP迁移到云下一代防火墙后，经过安全检测后再通过云专线回注到客户物理网络实现安全防护。

产品标杆项目-部分用户

天翼云

医疗行业

济宁市卫生健康委员会 Jining Municipal Health Commission

安国市医院

福建医科大学附属协和医院 Fujian Medical University Union Hospital

中山大学附属口腔医院 Hospital of Stomatology,SunYat-sen University

南岔市医院 团结 | 进取 | 精诚 | 创新

国药集团 SINOPHARM

内蒙古自治区人民医院 INNER MONGOLIA PEOPLE'S HOSPITAL

宁夏第五人民医院 The Fifth People's Hospital of Ningxia

政企行业

PICC 中国人保 湖南人保智慧气象灾害风控服务平台 Hunan People's Protection Intelligence Meteorological Disaster Wind Control Service Platform

新疆维吾尔自治区高级人民法院

西藏自治区人民政府 Cloud

重庆渝富资产经营管理集团有限公司 Chongqing Yufu Assets Management Group Co.,Ltd

TJE 天津能源 TIANJIN ENERGY | 天津津能易安泰科技有限公司 TIANJIN JINNENG EMPIRE TECHNOLOGIES CO., LTD.

乡零弓四

双良集团 SHUANGLIANG GROUP

中山产权交易网 ZHONGSHAN ENTERPRISES MERGERS AND ACQUISITIONS

ITercn 邮电人才

中化能源 SINOCHEM ENERGY

中化泉州石化有限公司 SINOCHEM QUANZHOU PETROCHEMICAL CO.,LTD.

中通服供应链管理有限公司 CHINA COMSERVICE SUPPLY CHAIN COMPANY

金融行业

广东农信 GDRC | 博罗农商银行 GUANGDONG BOLUO RURAL COMMERCIAL BANK

华融证券 HUARONG SECURITIES

陕西金融控股集团 SHAANXI FINANCIAL HOLDING GROUP

国家税务总局西藏自治区税务局 Tibet Autonomous Region Tax Service,State Taxation Administration

首创证券 Capital Securities

交通银行 BANK OF COMMUNICATIONS | 甘肃省分行 GANSU BRANCH

中国农业银行 AGRICULTURAL BANK OF CHINA

产品标杆项目(1/4)：医疗行业-济宁卫计委

项目需求及背景

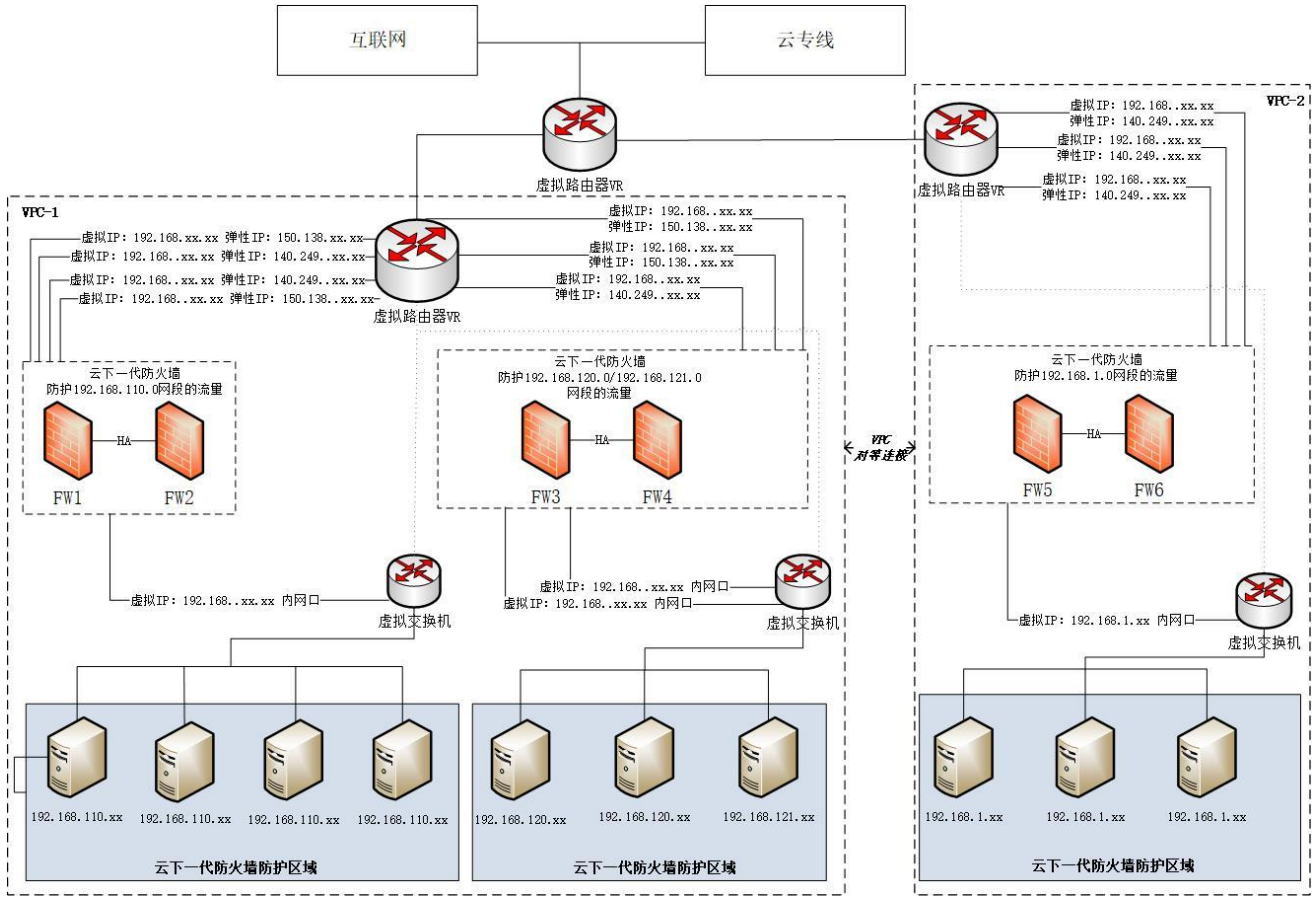
- 内外网隔离：医院有内外网之分，对外有OA、医院网站等等系统，对内有HIS、PACS、CIS等系统，这两套系统需要进行内外网隔离。
- 内网安全：云主机被植入后门，当内网主机失陷之后，黑客远程控制该主机进行病毒传播，获取更多失陷主机的控制权。

解决方案

- 按照部门、业务种类进行防火墙的安全防护范围划分，计划采用6台高级版的云下一代防火墙进行防护。
- 采用双机主备模式部署，在保证业务稳定的情况下重点突出网络的健壮性、可靠性。
- 入侵防御：防范外网对系统漏洞的深度挖掘并进一步获取权限。
- 病毒过滤：针对云主机内外互访时的操作进行病毒检测、阻止可疑行为以及破坏病毒文件。
- 带宽管理：按照客户需求进行业务之间的逻辑区分。

收益和价值

- 提高VPC业务系统环境的安全性，满足国家、相关行业的建设标准；
- HA高可靠性部署，有效保证业务的不中断，提高VPC环境的业务稳定性和可靠性；
- 云下一代防火墙可提供2-7层全方位安全防护，实现入侵防御、病毒过滤、攻击防护、带宽管理等安全功能；
- 通过云下一代防火墙，可以实时阻断来自互联网的网络攻击、主动探测和处置各种病毒木马威胁，为云平台中的主机提供全面的安全防护；



产品标杆项目(2/4)：政府行业-湖南省气象服务中心

项目需求及背景

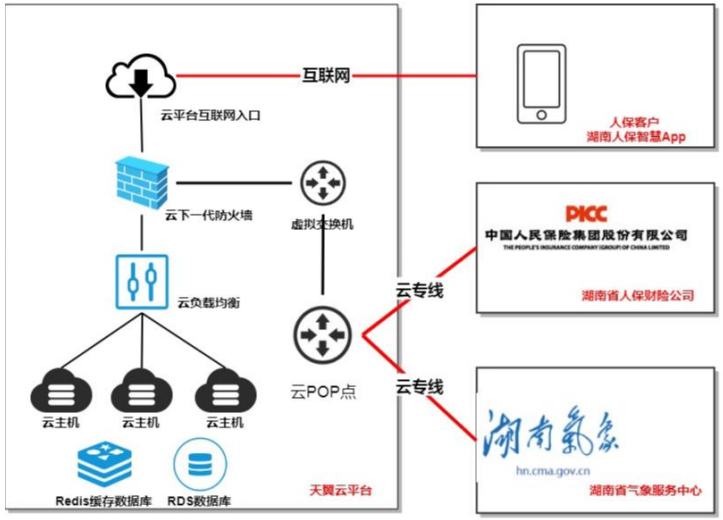
- 中国人保财险公司湖南分公司与湖南省气象局签订战略合作协议，需建设一个智慧气象风控服务平台，将湖南省气象突发事件预警信息发布平台与湖南省人保集团的风控服务平台对接，通过气象大数据将突发事件预警信息实时推送给人保客户，将灾害评估与防灾工作相结合，提升气象灾害预警信息在防灾减灾避灾增效中的作用。
- 风控服务平台为面向互联网的服务平台，同时需要与省人保和省气象服务器中心API接口互通，需要保障网络传输安全。
- 项目初期业务量不高，业务上量后需要快速进行扩容，保障业务平滑扩展。

解决方案

- 平台整体租用天翼云资源，通过两条云专线连接省气象服务中心接口和省人保风控服务平台接口，保障网络传输安全。
- 在云平台互联网出口部署云下一代防火墙，实时阻断来自互联网的网络攻击、主动探测和处置各种病毒威胁，保障业务平台的安全可靠。
- 业务前端使用云负载均衡进行业务分发，在业务量增大需要进行计算资源扩容时只需要增加云主机到负载均衡服务器组，业务架构不需要进行调整，保障应用平滑扩容。
- 采用天翼云RDS数据库主备版并开启数据自动备份功能，用户不需要自行维护数据库集群，为保障数据库的高可用及数据安全。

收益和价值

- 云墙部署简单，不影响网络拓扑，且安全防护能力业内领先；
- 提高VPC业务系统环境的安全性，满足国家、行业的建设标准；
- 通过云下一代防火墙，可以实时阻断来自互联网的网络攻击，为云平台中的主机提供全面的安全防护；
- 只用一台云墙就可满足VPC内所有云主机的攻击防护，入侵防御，DDOS攻击防护等安全功能需求，节约安全产品购买成本；



产品标杆项目(3/4)：企业行业-中通服供应链管理湖南分公司

项目背景及需求

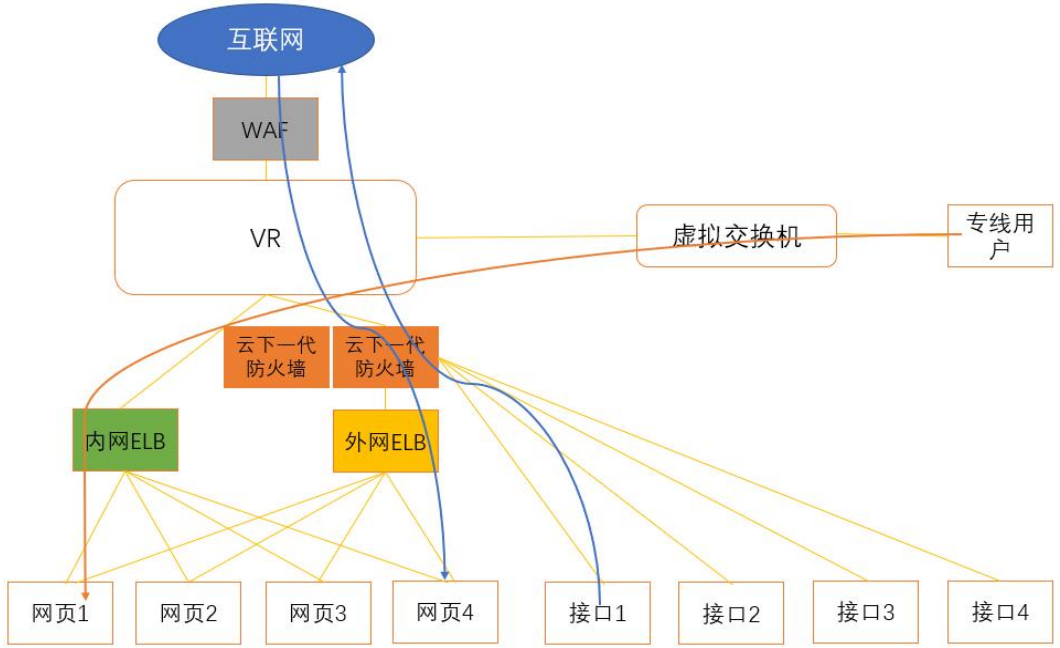
- 中通服供应链管理有限公司湖南分公司已经进行了域名备案，云平台中部署了数目众多的主机，提供网页服务、数据库服务、接口服务等；
- 云平台内流量既有外访内的流量，也有内访问的流量，还有云专线上来的流量；客户希望对进出互联网的流量进行安全防护，并在网页主机上获取访问网站的公网源IP；
- 备案域名解析的公网IP挂在外网ELB上，这个弹性IP不能更换。

解决方案

- 在云平台互联网出口部署两台云下一代防火墙，实现冗余部署，提高可靠性，由内访问互联网和由外访问云主机服务流量均经过云下一代防火墙的检测，配置SNAT和DNAT以及安全策略，开启安全功能，保障VPC环境的安全和业务的正常运行；
- 将外网ELB上的弹性IP换绑到防火墙上，实现外访内流量的检测和过滤，将接口主机上的弹性IP换绑到防火墙上，实现内访外流量的检测和过滤。

收益及价值

- 通过云下一代防火墙实现了域名备案网站的安全防护，并且不需要重新备案；
- 云下一代防火墙提供丰富的安全功能，实现2-7层全方位安全防护，保障客户网站及业务云主机的安全，保障业务持续稳定运行；
- 通过云下一代防火墙实现公网源IP的溯源，方便进行流量分析，云下一代防火墙提供多种日志记录，包括威胁日志、事件日志、配置日志、会话日志、NAT日志、URL日志等，方便客户进行运维审计。



产品标杆项目(4/4)：金融行业-广东博罗农村商业银行

项目需求及背景

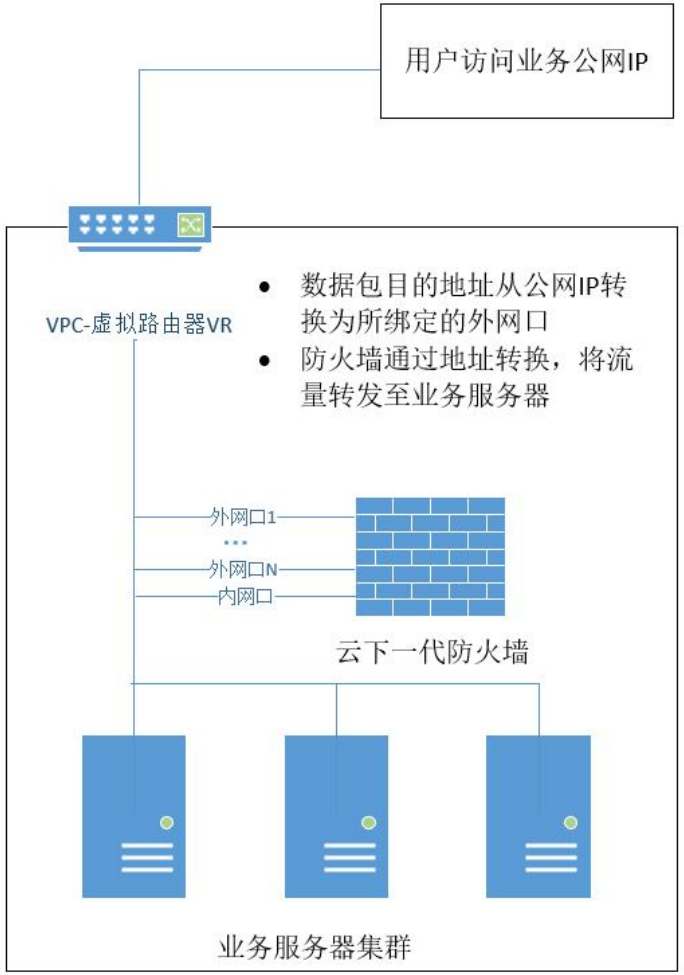
- 前端业务需要在云上部署，如直接暴露公网存在重大安全威胁
- 业务页面存在跳转到各页面的登录页面，评估此现象存在暴力破解的可能性。
- 在客户沟通之后采用业务与云下一代防火墙同时部署。

解决方案

- 部署1台标准版的云下一代防火墙位于业务云主机的前侧。
- 隐藏业务云主机的真实IP地址并禁止端口扫描、PING等前期探测手段。
- 入侵防御：防止通过异常访问手段进行敏感信息的获取。
- 访问控制：根据自定义的安全策略进行内外网的安全隔离。
- 地址转换：针对业务云主机的私有IP进行隐藏。

收益和价值

- 提高VPC业务系统环境的安全性，实现VPC环境的安全加固；
- 提供地址转换功能，满足外访内业务和内访外业务的地址转换需求；
- 云下一代防火墙提供丰富的网络安全功能，可对互联网流量进行监控统计，实现入侵防御、攻击防护、应用识别等功能，提供2-7层多维度的安全防护，保障关键业务正常运行。



感谢聆听！