绿盟下一代防火墙云服务(vNF)

技术白皮书

目录

一. 概述

随着虚拟化技术广泛应用，特别是公有云服务的大面积使用，越来越多的用户选择将业务放在公有云之上，享受方便、快捷、高效的云服务。但是由于传统安全架构无法满足虚拟化下灵活性和动态性要求，因此传统安全方案无法有效应对，因此云上客户的网络管理人员面临如下挑战：

- 大量应用直接复用同一标准协议的知名端口，或者直接承载在标准协议中。以协议和端口来辨别应用，进而进行网络访问控制的方式已失效。
- 威胁入侵多以外网攻击或内网感染为触发点，一台设备被攻陷或感染后，作为跳板或传染源对内网其他资产设备进行扩散和传播，引起内网泄密、资源占用等财产损失。
- 如何评估现网、尽早发现内网资产易受攻击的薄弱环节、填补漏洞、防患于未然，而将安全事件扼杀于事前，是较事中、事后等被动防范更加主动有效的安全防护措施。
- 如何在公有云提供网络安全能力和第三方安全厂商的虚拟安全设备之间进行选择，一般来说公有云会提供安全组、NAT 等边界隔离的能力，如何与第三方安全厂商的虚拟化设备结合？

绿盟下一代防火墙云服务(vNF)，是专门为公有云环境设计的网络安全产品，以虚拟化形态部署，适用于多种虚拟化平台，使管理员可以快速高效地调配和扩展防火墙。产品支持应用识别、入侵防御、内容过滤、URL过滤、VPN等，可以为用户提供L4-L7全面的安全服务。

二. 关键特性

2.1 专业的应用层防护

在充分考虑到现在及未来安全业务情景的前提下，绿盟下一代防火墙云服务(vNF)核心安全功能采用了高度一体化的架构设计方案，将所有的安全特性纳入到一体化的引擎中去。这样的一个明显优势是去除了传统 UTM 设备上各安全模块引擎间彼此独立，层层堆叠，每个引擎重复拆解数据包，彼此间没有任何传承配合，安全性能低下的冗余架构。同时，一体化安全引擎在系统中多核多进程并行执行，对网络海量数据进行实时、并发安全扫描和过滤，从而使产品安全性能有了一个质的飞跃，不仅是传统防火墙无法比拟，也从根本上解决了 UTM 设备安全模块开启，安全性能指数下降的传统顽疾。

结合公司在业界一贯知名的安全攻防能力，绿盟科技一体化安全引擎将其进行高度融合，从而确保用户网络安全高枕无忧，体现在：

- **入侵防护**

威胁入侵防护是绿盟科技在业界领先的传统优势之一，其特设的安全研究院，先后独立发现许多国际著名厂商（如 Microsoft、HP、CISCO、SUN、Juniper 等）40 多个重大安全漏洞，雄厚的威胁发现和响应能力保证了绿盟下一代防火墙云服务(vNF)在入侵防护规则和防御能力方面的领先。

绿盟下一代防火墙云服务(vNF)威胁特征库超过 3000 条，由绿盟科技安全研究院精心提炼，并经过了长期考验，能够主动防御已知和未知攻击，实时阻断各种黑客攻击，如缓冲区溢出、SQL 注入、暴力猜测、拒绝服务、扫描探测、非授权访问、蠕虫、僵尸网络等。广泛精细的安全防护保障用户免受安全损失。

同时，绿盟下一代防火墙云服务(vNF)能够全面抵御 ICMP Flood、UDP Flood、ACK Flood 等 D.o.S 攻击，阻挡或限制任何非法通信触发的带宽消耗，极大限度地减轻 D.o.S 攻击对网络带来的危害。

- **URL 过滤**

越来越多的病毒、木马等恶意代码将基于 HTTP 方式传播，新一代的 Web 威胁具备混合性、渗透性和利益驱动性，成为当前增长最快的风险因素。员工对互联网的依赖性使得企业网络更容易遭受到病毒攻击，导致用户信息受到危害，对公司数据资产和关键业务构成极大威胁。

绿盟下一代防火墙云服务(vNF)内置先进、可靠的 Web 信誉库，采用独特的 Web 信誉评价技术，在用户访问挂马等有安全风险的网页时，给予及时报警和阻断，从而有效防止安全威胁通过 Web 访问渗入到企业内部，保障了企业机密信息不泄露。

绿盟下一代防火墙云服务(vNF)拥有具备业界领先优势的 URL 分类库，包括 64 个类别数亿条 URL 条目，特有的“URL 数据云”突破了传统本地站点库解决方案的数量和准确性局限，为 URL 站点过滤服务提供了无可比拟的准确性和安全性。

- **内容过滤**

通过定义关键字，绿盟下一代防火墙云服务(vNF)可对网络传输中的网页、搜索、文件传输、邮件收发、论坛、服务器操作、即时通讯等应用的深层内容信息进行关键字过滤，并可根据用户需求，对匹配关键字的应用数据包进行检测、阻断、告警、记录和信息还原，从而实现了对内容的深度安全管理，避免用户机要信息、重要文件的外泄以及非法言论的传播等。

2.2 全面的应用识别能力

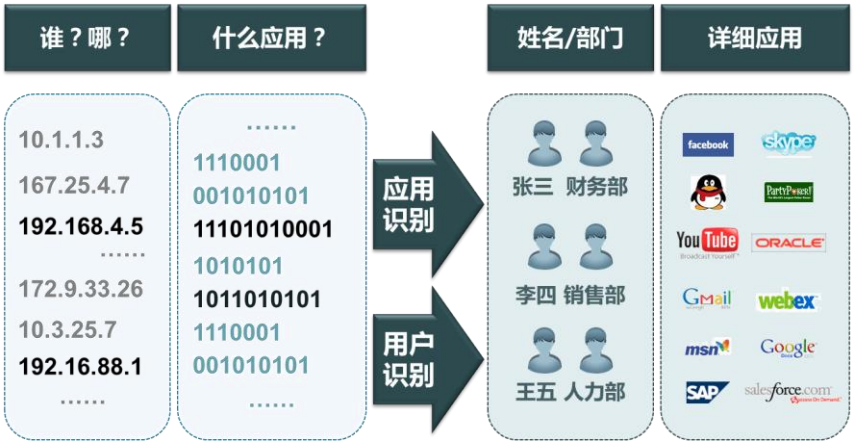

图 2.1 应用识别

应用识别是下一代防火墙技术的关键特征之一，绿盟下一代防火墙云服务(vNF)无论在可识别应用数，还是在应用服务上，均具有显著优势。绿盟下一代防火墙云服务(vNF)可识别

1000+种应用，并可辅助用户对这些应用进行高效管理和筛查，包括 5 维度分类组织、基于特性查询应用、自定义特殊应用等，让用户明显的感觉到绿盟下一代防火墙云服务(vNF)在应用识别和管理方面的专业性。

同时，绿盟科技拥有一支业界知名的，由资深安全专家组成的安全研究团队，他们长期不懈的跟踪前沿安全市场，保持着对最新网络应用和企业业务需求的提炼和积累，从而保证绿盟下一代防火墙云服务(vNF)的应用识别和安全库时时刻刻保持最高、最精确的应用和威胁识别率。

技术方面，绿盟下一代防火墙云服务(vNF)结合智能应用协议识别、高层应用特征匹配、动态流量及行为分析等多种技术，保证了对应用精准识别的技术优势，体现在：

- **智能应用协议识别**

应用协议识别是新一代网络安全产品的核心技术。传统防火墙，通过固定的协议端口映射表来判断流经的网络报文属于何种应用协议。但事实上，应用协议与端口是完全无关的两个概念。同样的端口可能会运行多种不同的应用，而应用也可能在任意一个指定的端口上运行，比如基于智能隧道的 P2P 应用（如各种 P2P 下载工具、IP 电话等），IMS（实时消息系统 如 MSN、Yahoo Pager），网络在线游戏等应用都可以运行在任意一个指定的端口，从而使传统的基于固定端口协议来区分应用的防火墙技术失效。

绿盟下一代防火墙云服务(vNF)采用特有的智能应用协议识别技术，通过动态分析网络报文中包含的协议特征，发现其所用协议，然后递交给相应的协议分析引擎进行处理，能够在完全不需要管理员参与的情况下，高速、准确地识别出通过动态端口或者智能隧道运用的真正应用。

- **应用特征匹配**

应用特征匹配主要检测各类已知应用，在全盘了解应用特征后，制作出相应的应用特征库及应用过滤器，对网络中传输的数据包进行高速匹配，确保能够准确、快速地检测到此类应用。

绿盟下一代防火墙云服务(vNF)装载权威的应用专家知识库，提供高品质的应用特征介绍和分析，能够精确识别各种复杂应用，并通过不断升级应用特征，保证第一时间最新应用的识别能力。

- **动态流量及行为分析**

除了对应用协议进行智能识别及对高层特征进行精确匹配，网络中的应用数据流在其他方面还具有特征、特异化的表现和踪迹，绿盟下一代防火墙云服务(vNF)针对应用的这部分特征也进行了跟踪、判断和识别，如基于应用数据包上下行流量分布差异化进行的分析识别，以及基于客户端/服务器访问模式、多协议转换尝试等动态行为进行的分析辨识。使得无论从静态到动态，从固定到智能，绿盟下一代防火墙云服务(vNF)在应用识别方面均做到了全面与精确。

2.3 细致的应用层控制

传统防火墙的访问控制或流量管理粒度粗放，只能基于 IP/端口号对数据流量进行一刀切式的禁止或允许。绿盟下一代防火墙云服务(vNF)基于卓越的应用和用户识别能力，对数据流量和访问来源进行精细化辨识和分类，使得用户可以轻易从同一个端口协议的数据流量中辨识出任意多种不同的应用，或从无意无序的 IP 地址中辨识出有意义的用户身份信息，从而针对识别出的应用和用户施加细粒度、有区别的访问控制策略、流量管理策略和安全扫描策略，保障了用户最直接、准确、精细的管理愿望和控制诉求。

例如，允许 HTTP 网页访问顺利进行，并且保证高访问带宽，但是不允许同样基于 HTTP 协议的视频流量通过；允许通过 QQ 进行即时通信，但是不允许通过 QQ 传输文件；允许邮件传输，但需要进行敏感信息过滤，如发现有泄密事件马上阻断，等等。

2.4 内网资产风险管理

绿盟科技下一代防火墙云服务，除了具备国际权威咨询机构 Gartner 所定义的下一代防火墙全部特性，不仅在新一代网络中保障用户的边界网络安全，防范“外敌”入侵，更首创性的提供内网资产风险识别功能，让用户对内网易受攻击资产进行风险提前评估和预警，双向安全，双向保障。即作为事中安全拦截设备，又作为事前风险防范设备，为用户在安全投资不变的情况下提供一举两得的加强安全效应。

2.5 完全涵盖传统防火墙功能

绿盟下一代防火墙云服务(vNF)兼容传统防火墙的所有功能特性，包括路由、交换、访问控制、流量管理、SNAT/DNAT、ISP 负载均衡、DDoS 防护、VPN、日志报表等，使用户原有成熟的安全解决方案可以无更改，平滑的过渡到绿盟下一代防火墙云服务(vNF)安全解决方案上来。

三. 典型应用

3.1 应用层防护

- **入侵防护**

绿盟下一代防火墙云服务(vNF)内置 4200+威胁特征库，并将威胁入侵分为 5 大类，分别是按攻击手段分类（如获取权限、信息收集类），按技术手段分类（如蠕虫、P2P），按流行程度分类（非常流行、中等流行），按危险程度分类，按服务类型分类等（如 WWW、FTP 事件等）。

绿盟下一代防火墙云服务(vNF)可防护远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等各种网络及应用攻击。同时支持用户自定义规则，建立规则组等功能。并能够对检测到的入侵事件实时告警、阻断、记录和提供统计报表。

- **URL 过滤**

绿盟下一代防火墙云服务(vNF)具有业界领先的基于云端的 URL 分类库，内含按照不同类型（如不良言论、色情暴力、网络“钓鱼”、论坛聊天等）划分，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤；

同时绿盟下一代防火墙云服务(vNF)内置的 Web 信誉库，通过对互联网站点资源（域名、IP 地址、URL 等）进行威胁分析和信誉评级，将含有恶意代码的网站列入 Web 信誉库，可有效阻挡用户对挂马等不良信誉网站的有意或无意访问，实现对终端用户的安全保护。

- **内容过滤**

通过内容安全关键字，绿盟下一代防火墙云服务(vNF)可对任意安全区域间交互的网页内容、搜索引擎信息内容、文件传输（文件名、格式、内容）、邮件收发（包括收发人、标题、内容、文件等）、论坛发言、服务器操作、以及即时通讯内容等进行基于内容关键字的准确检测、阻断、告警、记录和信息还原，实现深度内容安全管理与跟踪，避免用户机密信息、重要文件通过网络外泄，也避免了非法言论及不良信息的传播。

3.2 应用识别和可视化

绿盟下一代防火墙云服务(vNF)内置应用识别库，支持 1400+种应用识别。在配置界面上为用户提供应用列表，并可将应用进行 5 维度分类，包括按风险等级分类（1-5 级威胁度），按商业类别、子类别分类（如媒体类，图片视频子类），按实现技术分类（如 P2P），以及按照特征标签分类（如消耗带宽类，传输文件类应用等）。同时支持按照以上 5 维度的任意组合供用户对应用进行详细查询定位。

用户可以使用绿盟下一代防火墙云服务(vNF)随时了解当前网络正在发生什么。具体体现为，可实时了解当前网络中正遭受哪些威胁攻击（包括入侵攻击、病毒、恶意站点及敏感信息），以及相应的威胁等级、攻击数目等。

同时，用户可实时了解当前网络中一段时间以来各网络接口带宽使用情况，流量排名前十的应用以及流量使用排名前十的用户，并可实时互查应用与用户流量间的使用关系。

3.3 一体化策略与控制

用户可以使用绿盟下一代防火墙云服务(vNF)进行一体化策略的配置。基于安全引擎的一体化设计，绿盟下一代防火墙云服务(vNF)在配置界面上为用户提供了较传统防火墙和 UTM 完全不同的清晰和简捷的管理体验，即一体化配置策略。

一体化配置策略将传统五元组访问控制与具有下一代防火墙特征的用户识别、应用识别控制有机的结合起来，同时对其他防火墙产品一贯分离且重复的安全策略配置方式，进行了高度集中和融合。

在一条策略中即可全部或部分选择：入侵防护、防病毒、URL 过滤、内容过滤。免去用户以往在多个不同安全配置页面间频繁切换，重复配置的不便。其结果是在其它防火墙产品

上需要配置 5、6 条策略才能实现的功能，现在在绿盟下一代防火墙云服务(vNF)上，只需要一条策略即可完成，且逻辑上更加清晰简单，便于理解，极大的提高了管理易用性和可维护性，防止了繁琐配置引起的错误风险。

四. 典型部署

绿盟下一代防火墙云服务(vNF)部署简便，支持在 Vmware、KVM 等虚拟化平台上运行。用户可以根据网络建设的需求，进行调配和扩展防火墙，以满足虚化环境的动态要求。

4.1 VPC 内的子网之间防护或子网访问互联网

绿盟下一代防火墙云服务(vNF)可以将 VPC 内的子网逻辑隔离成不同的安全域，从而实现子网之间的防护或子网访问互联网的控制。

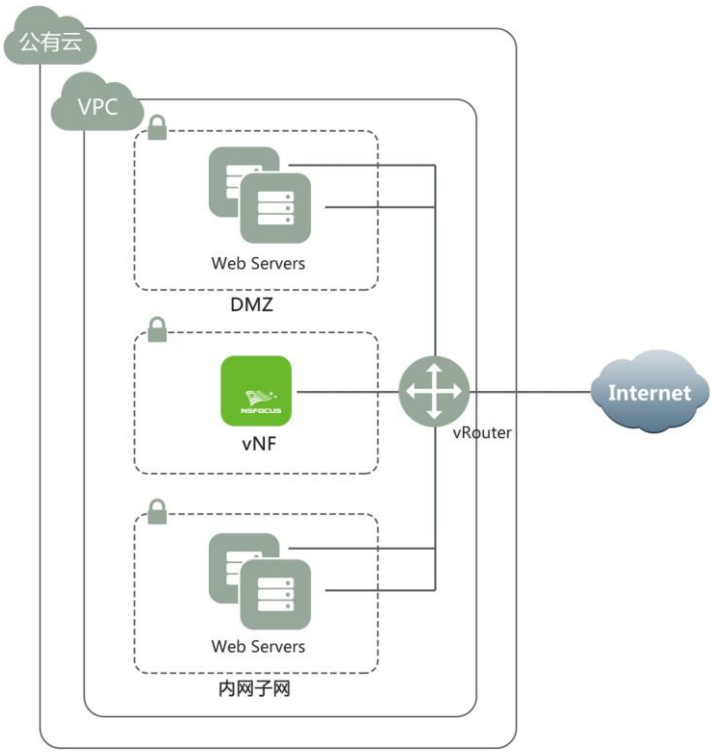

图 4.1 子网之间防护或子网访问互联网的示例拓扑

4.2 远程安全互联

VPC 与数据中心通过 IPSec VPN 互联，使得 VPC 内 VM 和数据中心的物理服务器可以互相访问；也可使用该方式将部署在不同公有云下，或同一公有云不同区域之间的 VPC 互联互通。

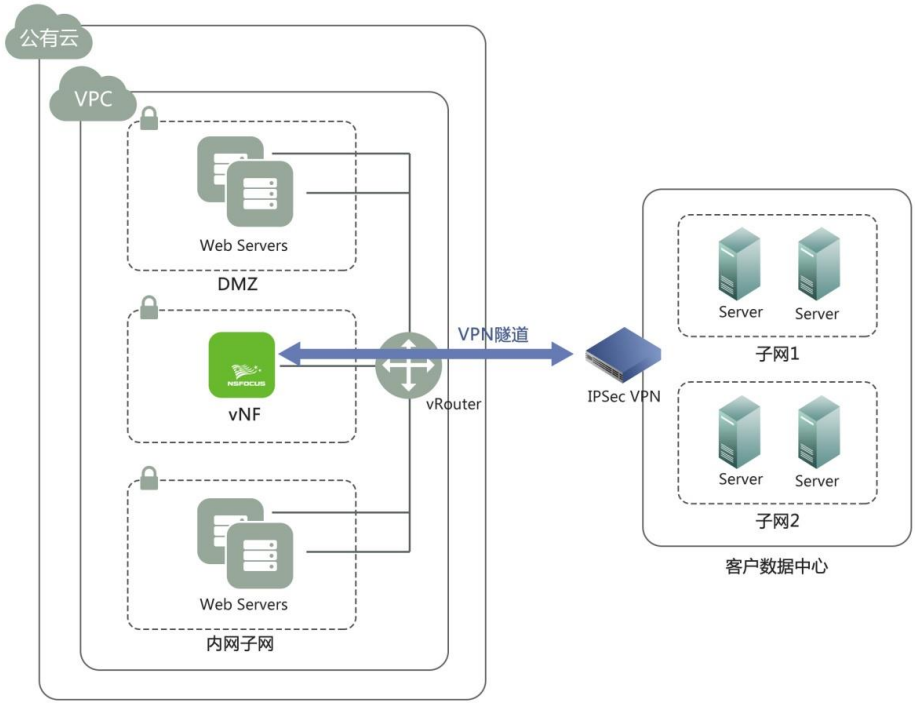

图 4.2 VPC 和客户本地数据中心互联的示例拓扑

五. 服务规格

5.1 基础级

绿盟下一代防火墙云服务(vNF)的基础级服务规格提供了安全防护相关的各项功能，并根据不同的防护性能提供四种版本。除安全防护能力之外，所有版本均提供绿盟科技 7x24 远程

技术支持服务，同时还提供了系统升级、规则升级相关服务，保证服务的安全防护能力能到及时更新。具体规格如下：

服务名称		绿盟下一代防火墙云服务(vNF)			
服务规格		标准版(50M)	标准版(100M)	标准版(200M)	标准版(1G)
功能	防火墙	√	√	√	√
	入侵防护	√	√	√	√
	IPSec VPN	√	√	√	√
	SSL VPN	√	√	√	√
	流量管理	√	√	√	√
	应用管理	√	√	√	√
	资产识别	√	√	√	√
性能	Realworld 吞吐量	50Mbps	100Mbps	200Mbps	1Gbps
	最大并发会话数	10 万	20 万	20 万	50 万
	每秒新增会话数	1 万	1 万	2 万	4 万
	SSL VPN 并发数	2	10	20	50
基础服务	远程技术支持服务	√	√	√	√
	产品系统升级服务	√	√	√	√
	产品规则升级服务	√	√	√	√
专家服务	上门产品安装与培训服务	——	——	——	——
	上门技术支持服务	——	——	——	——

5.2 专家级

专家级服务规格在基础级的服务规格之上，提供额外 1 次由绿盟专业安全工程师负责第一次服务部署和初始化安装，同时提供面对面的服务使用培训。之后在服务有效期内提供一次绿盟安全工程师上门技术支持服务。具体规格如下：

服务名称		绿盟下一代防火墙云服务(vNF)			
服务规格		增强版(50M)	增强版(100M)	增强版(200M)	增强版(1G)
功能	防火墙	√	√	√	√
	入侵防护	√	√	√	√
	IPSec VPN	√	√	√	√
	SSL VPN	√	√	√	√
	流量管理	√	√	√	√
	应用管理	√	√	√	√
	资产识别	√	√	√	√

性能	**Realworld 吞吐量**	50Mbps	100Mbps	200Mbps	1Gbps
	最大并发会话数	10 万	20 万	20 万	50 万
	每秒新增会话数	1 万	1 万	2 万	4 万
	SSL VPN 并发数	2	10	20	50
基础服务	远程技术支持服务	√	√	√	√
	产品系统升级服务	√	√	√	√
	产品规则升级服务	√	√	√	√
专家服务	上门产品安装与培训服务	1 次	1 次	1 次	1 次
	上门技术支持服务	1 次	1 次	1 次	1 次

5.3 阿里云中使用的建议虚机规格

服务名称	服务规格	AWS 下建议规格
绿盟下一代防火墙云服务(标准版)	标准版(50M)	**推荐 1：**ecs.sn1.medium vCPU：2；内存：4G；实例存储：10GB **推荐 2：**ecs.sn1ne.large（网络增强） vCPU：2；内存：4G；实例存储：10GB
	标准版(100M)	**推荐 1：**ecs.sn1.large vCPU：4；内存：8G；实例存储：10GB **推荐 2：**ecs.sn1ne.xlarge（网络增强） vCPU：4；内存：8G；实例存储：10GB
	标准版(200M）	
	标准版(1G)	**推荐 1：**ecs.sn1.xlarge vCPU：8；内存：16G；实例存储：10GB **推荐 2：**ecs.sn1ne.2xlarge（网络增强） vCPU：8；内存：16G；实例存储：10GB
绿盟下一代防火墙云服务(增强版)	增强版(50M)	**推荐 1：**ecs.sn1.medium vCPU：2；内存：4G；实例存储：10GB **推荐 2：**ecs.sn1ne.large（网络增强） vCPU：2；内存：4G；实例存储：10GB
	增强版(100M)	**推荐 1：**ecs.sn1.large

	增强版(200M)	vCPU：4；内存：8G；实例存储：10GB **推荐 2**：ecs.sn1ne.xlarge（网络增强） vCPU：4；内存：8G；实例存储：10GB
	增强版(1G)	**推荐 1**：ecs.sn1.xlarge vCPU：8；内存：16G；实例存储：10GB **推荐 2**：ecs.sn1ne.2xlarge（网络增强） vCPU：8；内存：16G；实例存储：10GB