H3C vFW 虚拟防火墙

产品概述

H3C vFW 产品（简称 vFW）是一款功能强大的软件安全产品，是 H3C 虚拟多业务安全网关解决方案的重要组件。

vFW 产品支持多种虚拟平台，基于专业的 H3C Comware V7 平台，能够监控和保护虚拟环境的安全，避免虚拟化环境与外部网络遭受内外部威胁的侵害，为虚拟化数据中心和云计算网络带来全面的安全防护，帮助企业构建完善的数据中心和云计算网络安全解决方案。

在安全功能方面， vFW 为用户提供了全面的安全防范体系和远程安全接入能力，支持攻击检测和防御、NAT、ALG、ACL、安全域策略，能够有效的保证网络的安全；采用 ASPF（Application Specific Packet Filter）应用状态检测技术，可对连接状态过程和异常命令进行检测，提供多种智能分析和管理手段，支持多种日志，提供网络管理监控，协助网络管理员完成网络的安全管理；支持多种 VPN 业务，如 L2TP VPN、GRE VPN、IPSec VPN、SSL VPN 等。

产品特点

领先的专业网络安全平台

基于业界领先的 Comware V7 平台：

- 丰富的网络和安全功能，能够满足企业分支及公有云中多租户环境的网络安全需求；
- 控制平面和数据平面分离，专门为虚拟环境优化的多核数据转发，更能充分利用计算资源；
- 模块化的体系架构，开放的网络平台，允许网络按需运行和控制，更容易实现 NFV/SDN 落地；
- 和物理网络设备采用统一的软件平台，提供相同的功能特性和一致的管理界面；

超轻量级部署

提供超轻量级部署体验：

- 适合在公有云中部署，实现零运输、零布线，加快业务的部署；
- 支持 VMware ESXi、Linux KVM、H3C CAS 等主流虚拟化平台，充分发挥虚拟化的优势，实现快速部署、批量部署、镜像备份、快速恢复，并且能够灵活迁移；
- 提供 ISO、OVA、IPE 等多种发布格式，适应不同虚拟化平台部署；
- 支持虚拟机管理平台、网管平台及本地等多种工具进行灵活部署；

超强业务弹性

提供超强业务弹性：

- 支持 VMware ESXi、Linux KVM、H3C CAS 等主流虚拟化平台，无缝适应用户的部署环境；
- 允许企业在虚拟化环境中搭建企业网络，可以按需动态地调配和管理网络资源及服务。例如，可以根据需要灵活调整网口数量和类型，而无需采购新硬件网卡；

- 通过动态调整虚拟机资源和 License，即可实现软件功能的平滑升级、设备性能的按需提升，随时满足业务增长需求；

完善的安全保障

防火墙过滤

- 支持包过滤。借助报文中优先级、TOS、TCP 或 UDP 端口等信息作为过滤参考，通过在接口输入或输出方向上使用标准或扩展访问控制规则，可以实现对数据包的过滤。同时，还可以按照时间段进行过滤；
- 支持应用层状态包过滤（ASPF）功能。通过检查应用层协议信息（如 FTP、HTTP、SMTP、RTSP 及其它基于 TCP/UDP 协议的应用层协议），并监控基于连接的应用层协议状态，动态的决定数据包是被允许通过防火墙或者是被丢弃；
- 支持丰富的攻击防范技术。包括：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范，还包括针 SYN Flood、UDP Flood、ICMP Flood 等常见 DDoS 攻击的检测防御；
- 支持多种 VPN 业务，如 L2TP VPN、IPSec VPN、GRE VPN 等，可以针对客户需求通过拨号、租用线及 VLAN 或隧道等方式接入远端用户，构建 Internet、Intranet、Access 等多种形式的 VPN。结合防火墙、AAA、NAT、及多种 QoS 等技术，防火墙可以确保在开放的 Internet 上实现安全、可靠的专用私有网络；
- 支持安全区域管理。可基于接口、VLAN 划分安全区域；
- 支持静态和动态黑名单；
- 支持丰富的路由协议。支持静态路由、策略路由，以及 RIP、OSPF 等动态路由协议；

NAT 应用

地址转换 NAT（Network Address Translation）又称地址代理，将内部网络主机的 IP 地址和端口号替换为外部网络地址和端口号，有效控制内部网络和外部网络之间的访问，不仅节约了宝贵的 IP 地址资源，并且为内部主机提供“隐私”保护。

- 提供多对一、地址池、ACL 控制等地址转换方式，在一个接口上支持多个不同的地址转换服务，通过内部服务器可以向外提供 FTP、Telnet 和 WWW 等服务，实现公网和私网混合地址解决方案；
- 除提供一般 NAT 功能以外，还提供针对多种应用协议，如多媒体应用（VOIP、视频）：H.323、RAS、SIP、SCCP、RTSP，VPN 应用 PPTP，常用的应用 FTP、TFTP、DNS、NBT、ICMP、DNS、ILS 的 NAT ALG 功能；

安全管理

- 提供各种日志功能，包括攻击实时日志、黑名单日志、会话日志、NAT 日志功能，能够有效的记录网络情况，从而为分析网络状况，防范网络攻击提供依据；
- 通过 H3C iMC 实现统一管理，集安全信息与事件收集、分析、响应等功能为一体，解决网络与安全设备相互孤立、网络安全状况不直观、安全事件响应慢、网络故障定位困难等问题，使 IT 及安全管理员脱离繁琐的管理工作，极大提高工作效率，能够集中精力关注核心业务；
    - 基于先进的深度挖掘及分析技术，为用户提供集中化的日志管理功能，并对不同类型格式（Syslog、二进制流日志等）的日志进行归一化处理。同时，采用高聚合压缩技术对海量事件进行存储，并可通过自动压缩、加密和保存日志文件到 DAS、NAS 或 SAN 等外部存储系统，避免重要安全事件的丢失；
    - 提供丰富的报表，主要包括基于攻击、应用的报表、基于网流的分析报表等；
    - 支持报告定制，定制内容包括数据的时间范围、数据的来源设备、生成周期以及输出类型等；

安全认证

- 支持用户身份管理，不同身份的用户拥有不同的命令执行权限，可以防止低级别权限用户非法获取或修改配置信息等；

- 视图分级保护。由于不同身份的用户拥有的配置权限不同，低级别用户不能进入更高级的视图；
- 支持基于RADIUS（Remote Authentication Dial-In User Service）的AAA（Authentication，Authorization，Accounting）服务，可以与RADIUS服务器配合实施对接入用户的验证、授权和计费安全服务，防止非法访问；
- 支持基于PKI/X.509的证书认证功能；
- 路由协议OSPF、RIP2都具有MD5认证功能，确保所交换路由信息的可靠性；

丰富的VPN接入能力

- L2TP VPN

L2TP为目前使用最广泛的VPDN（Virtual Private Dial Network）隧道协议。L2TP协议提供了对PPP链路层数据包的通道（Tunnel）传输支持，支持L2TP多域。

- GRE VPN

GRE是第三层隧道协议，在协议层之间采用了一种被称之为Tunnel（隧道）的技术，在一个Tunnel的两端分别对数据报进行封装及解封装。

- IPSec VPN

IPSec（IP Security）协议族是IETF制定的一系列协议，它为IP数据报提供了高质量的、可互操作的、基于密码学的安全性。特定的通信方之间在IP层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。IPSec通过AH（Authentication Header，认证头）和ESP（Encapsulating Security Payload，封装安全载荷）这两个安全协议来实现上述目标。IPSec可以通过手工方式建立安全联盟，也可以通过IKE方式（Internet Key Exchange，因特网密钥交换协议）自动为IPSec提供自动协商交换密钥、建立和维护安全联盟的服务。IPSec协议为对信息安全要求较高的用户提供了一个安全的VPN解决方案。通常情况下，与L2TP协议和GRE协议等相结合使用。

- SSL VPN

首先，SSL协议是一种加密协议，可以很好地保证数据传输的私密性和完整性。其次，SSL协议还是一种工作在TCP协议层之上的协议。使用SSL进行通讯，不改变IP报文头和TCP报文头，因而SSL报文对NAT和防火墙来说都是透明的，SSL VPN的部署不会影响现有的网络。这样用户从任何地方上网，只要能接入Internet，就能使用SSL VPN。另外，SSL加密协议受到了目前决大多数软件平台的支持。常用的操作系统Windows、Linux，浏览器IE、Firefox等都支持SSL。SSL VPN以其简单易用的安全接入方式、丰富有效的权限管理，跨平台、免安装、免维护的客户端而成为远程接入市场上的新贵。

配合SDN控制器实现智能网络

配合SDN控制器，能够实现：

- vFW基于用户配合VNF Manager实现一键部署及删除；
- 支持VxLAN 三层网关功能；
- 通过控制器实现服务链功能；
- 支持netconf、openflow流表等多种SDN协议；

产品规格

属性	说明	
软件包	H3C vFW1000 软件、H3C vFW2000 软件 支持 ISO, OVA, ,QCOW2, IPE 四种发布格式	
虚拟平台	VMware ESXi Linux KVM H3C CAS	
虚拟机	虚拟机资源最小要求： 1 个 vCPU (主频 2.0 GHz 以上) 1GB 内存 8GB 硬盘 至少两个虚拟网口	
	虚拟网卡类型：E1000，VMXNET3，VirtIO，Intel 82599VF	
	最大支持 16 个虚拟网口	
License	基于虚拟 CPU 数量和时间的控制（1vCPU、4vCPUs、8vCPUs / 1 年、3 年、永久） 基于物理 CPU 数量和控制（1CPU、2CPUs、4CPUs） 支持试用 License	
网络安全性	AAA 服务	Portal 认证 RADIUS 认证 HWTACACS 认证 PKI/CA（X509 格式）认证 域认证 CHAP 验证 PAP 验证
	防火墙	安全区域划分，不同安全域默认拒绝 攻击防范：可以防御 Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法超大 ICMP 报文、地址扫描、端口扫描、SYN Flood、UPD Flood、ICMP Flood 等多种恶意攻击 基础和扩展的访问控制列表 基于接口的访问控制列表 基于时间段的访问控制列表 动态包过滤 ASPF 应用层报文过滤 静态和动态黑名单功能 MAC 和 IP 绑定功能 基于 MAC 的访问控制列表 连接数限制
	NAT	支持多个内部地址映射到同一个公网地址 支持多个内部地址映射到多个公网地址 支持内部地址到公网地址一一映射 支持源地址和目的地址同时转换 支持外部网络主机访问内部服务器 支持内部地址直映射到接口公网 IP 地址

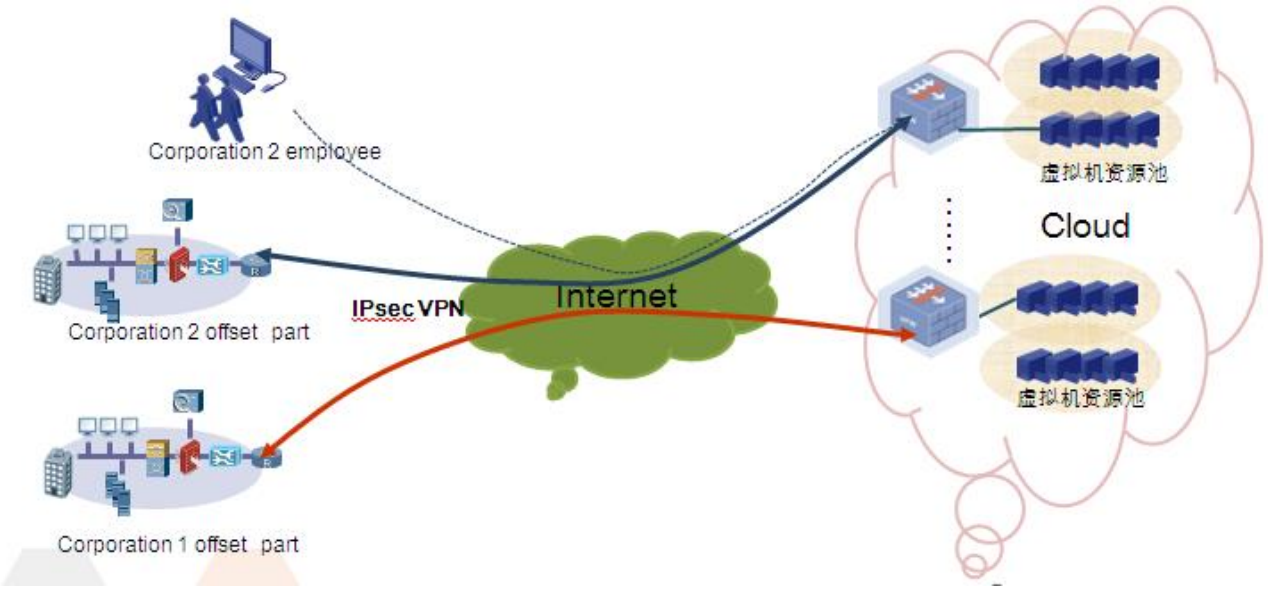
属性	说明	
		支持 DNS 映射功能 可配置支持地址转换的有效时间 支持多种 NAT ALG，包括 DNS、FTP、TFTP、PPTP、H.323、SIP、RSH、ILS、MSN、NBT 等
VPN	L2TP VPN	支持根据 VPN 用户完整用户名、用户域名向指定 LNS 发起连接 支持为 VPN 用户分配地址 支持进行 LCP 重协商和二次 CHAP 验证
	IPSec/IKE	支持 AH、ESP 协议 支持手工或通过 IKE 自动建立安全联盟 ESP 支持 DES、3DES、AES 多种加密算法 支持 MD5 及 SHA-1 验证算法 支持 IKE 主模式及野蛮模式 支持 NAT 穿越 支持 DPD 检测
	GRE VPN	
	SSL VPN	支持端口转发接入 支持网络扩展接入 支持 WEB 代理接入 支持无改写 WEB 代理接入 支持支持 NETCONF 支持认证功能：本地认证/Radius 认证/LDAP 认证/AD 认证/证书认证 支持 IRF/资源管理/动态授权/日志审计 支持个性化/虚拟化 浏览器支持: IE8 及以上/Firefox 25 及以上/Chrome 32 及以上/Safari 7 及以上
网络互连	局域网协议	三层以太网接口/子接口 ARP VLAN Terminating
	链路层协议	PPPoE Client
网络协议	IP 服务	Forwarding/Fast Forwarding TCP, UDP, IP Option Ping, Trace DHCP Server, DHCP Relay, DHCP Client DNS Client, DNS Proxy, DDNS FTP Server, FTP Client, TFTP Client Telnet Server. Telnet Client NTP/SNTP
	IP 路由	静态路由 RIP v1/2 OSPF 策略路由
高可靠性	支持 VRRP/VRRPv3 支持 BFD	高可靠性

属性	说明	
配置管理	命令行接口	通过 Console 口进行本地配置 通过 Telnet 或 SSH 进行本地或远程配置 配置命令分级保护，确保未授权用户无法侵入设备 详尽的调试信息，帮助诊断网络故障 User-interface 配置，提供对登录用户多种方式的认证和授权功能。
	支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2c 支持 NETCONF, RMON, Syslog, NQA, sFlow, NetStream, EAA	
	支持 H3C iMC 智能管理中心	
IPv6	IPV6 业务	TELNET/ICMP 域名解析 DHCP 中继 DHCP 客户端 IPv6 ND, IPv6 PMTU, IPv6 FIB, IPv6 ACL
	IPV6 路由	静态路由 策略路由 RIPng OSPFv3
	IPV6 安全	IPV6 包过滤 IPV6ASPF IPV6 域间策略 IPV6 攻击防范

典型组网

数据中心租户网关应用

在数据中心环境中，作为租户专用的综合业务网关，提供 VPN 隧道，为不同租户提供安全接入；同时，作为出口网关，防范各种来自外部的攻击，也可作为内网访问控制设备隔离不同安全等级的区域，实现对网络流量的安全防护；



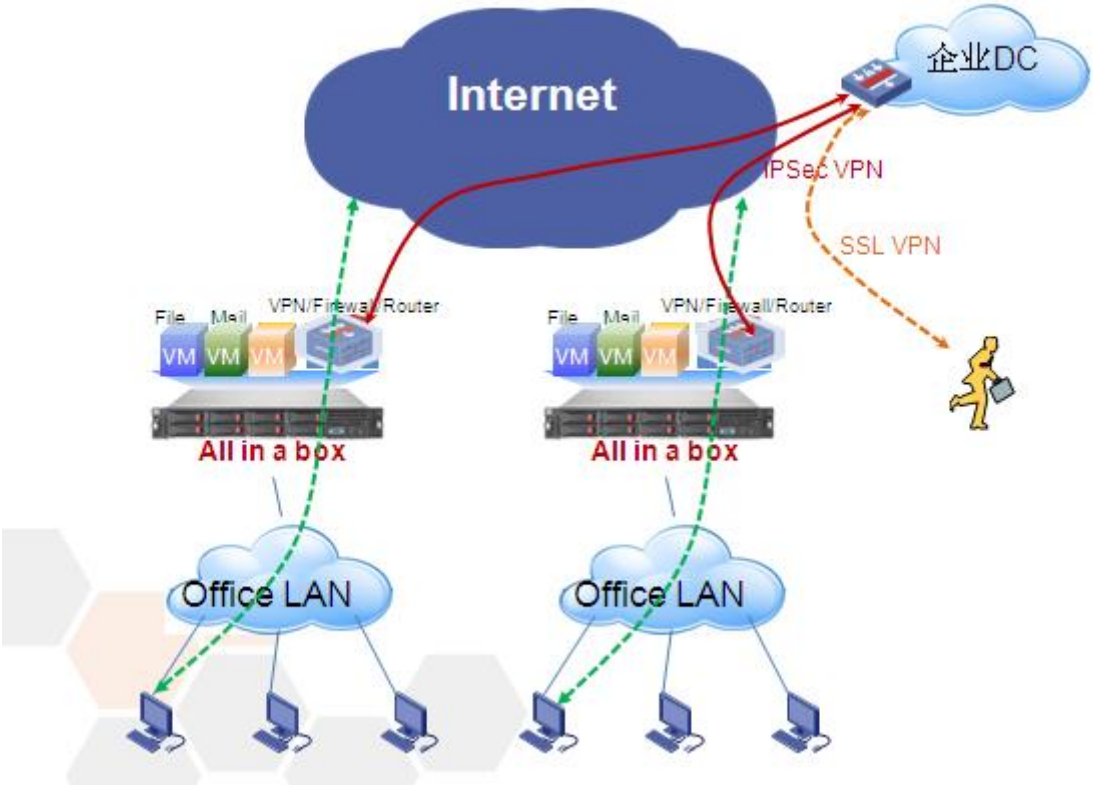
租户网关应用典型组网

- 精简网络基础设施，直接利用服务器，便于租户自行维护；
- 业务弹性扩展，性能可动态调整，管理高效
- 支持分区域安全控制
- 支持 NAT，支持多种 ALG
- 通过报文检测并阻止非法入侵。
- 支持多种攻击防范技术。
- 支持黑名单过滤。
- 支持通过 TCP 代理实现 Syn Flood 防攻击。
- 支持流量日志及攻击告警日志。

企业分支综合网关

在企业分支中，vFW1000 作为企业分支综合网关，部署在标准服务器中，负责接入 Internet，为分支出口提供专业的安全防护；同时支持与企业数据中心建立 VPN 连接(包括 IPsec VPN，L2TP，GRE),确保接入安全。

精简企业分支基础设置，易于管理；支持企业应用部署在同一硬件平台上，满足计算和网络设备融合的需求，



企业分支综合网关典型组网

订购信息

vFW1000 软件可以免费下载进行安装，需要购买 License 进行使用。

项目	描述
LIS-vFW1000-C1-Y1	H3C SecPath vFW1000 授权函(Comware V7,1vCPU,1 年授权)
LIS-vFW1000-C1-Y3	H3C SecPath vFW1000 授权函(Comware V7,1vCPU,3 年授权)
LIS-vFW1000-C1	H3C SecPath vFW1000 授权函(Comware V7,1vCPU,永久授权)
LIS-vFW1000-C4-Y1	H3C SecPath vFW1000 授权函(Comware V7,4vCPU,1 年授权)
LIS-vFW1000-C4-Y3	H3C SecPath vFW1000 授权函(Comware V7,4vCPU,3 年授权)
LIS-vFW1000-C4	H3C SecPath vFW1000 授权函(Comware V7,4vCPU,永久授权)
LIS-vFW1000-C8-Y1	H3C SecPath vFW1000 授权函(Comware V7,8vCPU,1 年授权)
LIS-vFW1000-C8-Y3	H3C SecPath vFW1000 授权函(Comware V7,8vCPU,3 年授权)
LIS-vFW1000-C8	H3C SecPath vFW1000 授权函(Comware V7,8vCPU,永久授权)

vFW2000 软件可以免费下载进行安装，需要购买 License 进行使用。

项目	描述
LIS-vFW2000-C1	H3C SecPath vFW2000 服务器授权函(Comware V7,1CPU,永久授权)
LIS-vFW2000-C2	H3C SecPath vFW2000 服务器授权函(Comware V7,2CPUs,永久授权)

项目	描述
LIS-vFW2000-C4	H3C SecPath vFW2000 服务器授权函(Comware V7,4CPUs,永久授权)

新华三技术有限公司

北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504