

★完全公开

# 网神 SecGate3600 防火墙

## NSG3300-5620-F

# 白皮书

地址：北京市西城区西直门外南路26号院1号

邮编：100044

# 1. 产品概述

## 1.1 产品简介

在信息化飞速发展的今天，网络形势正发生着日新月异的演变，层出不穷的新型威胁冲击着现有的安全防护体系。传统的安全设备，一是以本地规则库为核心，无法有效检测已知威胁；二是没有数据智能，无法感知未知威胁；三是没有联动智能，无法对网络进行协同防御。面对诸如 0-day、APT 及未知威胁等越来越多样化和层次化的攻击，逐渐变得力不从心。归根结底，现在的安全和产品体系还在用单机的、私有的思路来解决网络的、公有的已知威胁。而面对未知的安全威胁，我们不能再孤军作战，而必须是协同共享。

## 1.2 产品形态及构架

产品名称	网神 SecGate 3600 防火墙系统 v3.6.6.0
产品型号	NSG3300-5620-F
电源	1+1 交流冗余电源
风扇	2+1 冗余风扇
部件	风扇、电源等部件支持热插拔
整机三层单向吞吐量	160Gbps
最大 TCP 并发连接数（条）	40M
新建 TCP 连接数（每秒）	1500K
IPsec 吞吐量	41Gbps
IPsec 隧道数	210000
整机端口	2 个 100G 光口，4 个 40G 光口，24 个万兆光口，8 个千兆光口，8 个千兆电口；
CPU 核数	24
内存	64GB
1000Base-TX 接口	支持提供

Ethernet 端口	支持 MTU jumbo frame, MTU 可配置修改。
维保	原厂 5 年 7*24 小时保修

## 2. 产品性能和功能

1、包转发能力 (Mpps): 指设备每秒能处理的 64 字节最小报文数量, 单位为百万包/秒 (Mpps)。

计算公式:  $\text{包转发率} = (\text{端口总带宽 (bps)} / ((64+20) \times 8)) \times 10^{-6}$

说明: 64 字节报文: 含 20 字节的帧间隙 (IFG) 加前导码, 实际传输需按 84 字节计算。吞吐量 (Gbps): 指实际有效数据传输速率, 不考虑协议开销。

计算公式:  $\text{吞吐量} = \text{端口数量} \times \text{单个端口速率 (Gbps)}$

NSG3300-5620-F 64 字节单向吞吐量为 40Gbps, 按照包转发率计算公式:  $(40\text{Gbps}) / ((64+20) \times 8) \times 10^{-6} = 59\text{Mpps}$ , 即单向包转发能力为 59Mpps。

2、在使用 2 个 100G 接口下进行 RFC 2544 单向吞吐量在 1518 字节下测试吞吐量为 160Gbps, 64 字节小包下板卡 PPS 为 59Mpps, 设备在满配置和多功能开启的情况下, 所有端口达到线速转发。

3、NSG3300-5620-F 在硬件设备 2 口 100G 下, CPU 负载 95% 环境下:

包大小 64 字节, 吞吐 40Gbps, 延时小于 28.101us;

包大小 512 字节, 吞吐 160Gbps, 延时小于 32.320us;

包大小 1518 字节, 吞吐 160Gbps, 延时小于 38.319us。

### 2.1 基础组网功能

1. 部署模式: 支持路由模式、透明模式、交换模式、混合模式以及旁路模式接入。

2. 路由特性: 默认路由、静态路由、策略路由、支持 RIP、RIPng、OSPF、

BGP 等动态路由。

3. IP 协议：支持 IPV4、IPV6 双栈。
4. NAT：支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式。
5. 负载均衡：支持基于 IP、ISP、应用、用户、服务等多链路负载均衡，支持 DNS 流量的负载均衡，支持基于服务器地址的负载均衡；支持 IPSec VPN 的多链路备份和负载。
6. 网络服务：支持 DHCP 服务器、DNS 透明代理、ARP 代理等网络服务。
7. VPN：支持 IPSec VPN、SSL VPN、L2TP、PPTP、GRE，IPSecVPN 支持国密算法；SSL VPN 支持 Windows 客户端、安卓客户端和 IOS 客户端；DS-Lite 支持作为 B4 和 AFTR。
8. 虚拟系统：支持虚拟系统路由、交换、监控、审计、安全、防护等全隔离。
9. 高可靠性：支持双机热备功能，支持路由和透明模式下的“主-备”、“主-主”模式，支持接口联动，链路探测。
10. LLDP 功能：可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息，如设备配置和设备识别等详细信息。

## 2.2 精细化访问控制功能

1. 访问控制：支持基于 IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制，支持一条安全策略配置应用控制、入侵防护、URL 过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，并支持安全策略的快速检索，冗余策略分析，命中时间分析和安全策略推荐。
2. 行为管控：支持对 HTTP、SMTP、POP3、IMAP、FTP、TELNET 协议进行细粒度的控制，过滤不受信任的网络行为。
3. 用户认证：支持基于 web 的无客户端方式的用户认证，具备集成 AD 活动目录、LDAP、RADIUS 的第三方认证。
4. 文件过滤：不基于后缀名方式实现对文档、压缩、归档三大类共 30

多种常用文档类型过滤。

5. 邮件过滤：支持对邮件收发件人进行过滤，基于 RBL 黑名单及自定义 IP 地址黑名单两种方式的反垃圾邮件支持。

6. URL 过滤：预置 133 类 URL 资源库，可手动离线或自动在线进行更新升级，支持 URL 云查询，支持云端 URL 查询分析，支持自定义 URL 过滤。

7. 内容过滤：实现 HTTP、FTP、POP3、SMTP、IMAP 五种应用协议的双向内容传输过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义。

8. 带宽管理：支持根据 IP 地址、用户、服务、应用、时间等信息划分虚拟 QoS 通道进行带宽管理，支持多层次调度类嵌套的最大带宽限制和最小带宽保证。

9. 流量编排：支持流量编排功能，支持配置管理多种物理网元，包含：WAF、IPS、DDOS、天眼等多种设备，并且支持对网元做健康检查；支持基于源安全域、目的安全域、源地址、目的地址、服务、应用、VLAN、服务链、流量方向的引流策略，并且可以显示引流策略的命中数；支持基于串接链和旁路连的服务链管理功能；支持多种负载均衡算法，包括源地址哈希、源目的地址哈希、加权源地址哈希、加权源目地址哈希、加权地址端口哈希、轮询和权重轮询。

10. 黑白名单：支持地址白名单；支持基于时间维度的 IP 或 MAC 的黑名单设置；支持域名黑白名单，域名支持通配符\*。

11. IP-MAC 绑定：支持基于安全域的 IPv4 和 IPv6 的 IP-MAC 绑定，支持 IP-MAC 探测；支持基于安全域的 IPv4 和 IPv6 的 IP-MAC 未绑定策略，对未绑定到 IP-MAC 绑定列表中的 IP 地址，可自定义允许访问还是禁止；支持 IP-MAC 探测，对探测结果进行绑定；支持跨三层 IP-MAC 探测，对探测结果进行绑定。

12. 资产准入策略：资产准入策略支持基于 IP 地址和资产类型对资产进行准入控制。

13. 资产黑白名单：支持添加、导入资产黑名单和资产白名单。

14. 共享接入管理：支持共享接入检测和共享接入管理。

## 2.3 一体化威胁防护功能

1. 攻击防护：支持攻击防护类型包括：Flood（SYN Flood、ICMP Flood、UDP Flood、IP Flood）、恶意扫描（禁止 tracert、IP 地址扫描攻击、端口扫描）、欺骗防护（IP 欺骗、DHCP 监控辅助检查）、异常包攻击（Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片、NTP Monlist）、ICMP 管控（禁止 ICMP 分片、禁止路由重定向报文、禁止不可达报文、禁止超时报文、ICMP 报文大小限制）、应用层 Flood（DNS Flood、HTTP Flood、NTP Query Flood、NTP Reply Flood、SIP Flood）、SYN Cookie。

2. 病毒防护：搭载人工智能引擎，能免疫 90% 以上的加壳和变种病毒，并支持病毒云查杀技术对 HTTP、FTP、SMTP、POP3 和 IMAP 流量进行病毒查杀。

3. 本地威胁情报检测：支持威胁情报库自动及手动升级，防火墙威胁情报数量为 4 万以上。

4. 入侵防御：目前可识别并阻断 7000 余种漏洞入侵和间谍软件，该数量后续会持续增加；支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL 注入、WEB 攻击、弱口令扫描等入侵行为防御，支持生成动态策略。

## 2.4 可视化智能管理功能

1. 设备管理：支持 Web 界面（Http、Https）和命令行界面（SSH、Console、CLI）。

2. 管理权限：支持超级管理员、策略管理员和审计管理员三权分立管理，支持自定义管理员权限。

3. 日志输出：支持流量日志、威胁日志、域名日志、URL 过滤日志、邮件过滤日志、行为日志等多维度中文可视化分析和日志外发，并支持基于 IP、用户、接口、地区、应用等多达 90 多种过滤条件模糊搜索自定义时间段内的历史日志。

4. 统计分析：支持按应用、IP、用户等类型对相应类型的字节数、会话

数进行在指定时间范围内进行排序，支持基于接口、安全域的新建连接数、并发连接数的历史统计。支持基于网络中的流量趋势及增长应用、下降应用、带宽消耗、威胁的排行统计。并支持威胁地图，帮助用户了解网络中威胁基于地理位置的分布的风险。

5. 监控分析：支持会话监控、用户监控、资产监控、路由监控、系统资源监控。

## 2.5 协同防御功能

1. 终端联动：智慧防火墙可以与奇安信天擎终端安全管理系统进行联动，增强防火墙对应用特征及木马特征的识别。

2. 天眼联动：支持与天眼系统联动，防火墙支持发送常用协议头部信息给天眼，支持加密传输方式，天眼可以向防火墙下发域名、URL、恶意 IP 等处置策略，支持自动处置和人工处置。

3. 天眼沙箱联动：防火墙支持与天眼威胁文件鉴定器（沙箱）联动，进行文件静态检测和动态检测，从而可以识别出未知威胁文件。

4. 蜜罐联动：支持与蜜罐、天眼分析中心联动，蜜罐进行威胁检测，天眼分析中心进行威胁分析、下发威胁处置策略。

5. 奇安信安全云联动：防火墙支持与奇安信安全云联动，通过奇安信安全云，云防进行病毒云查杀、URL 云识别、云沙箱、应用云识别、威胁情报云检测，奇安信安全云应急响应通知，支持防火墙向奇安信安全云，云镜上传日志，并通过云端威胁情报进行威胁检测。

6. NGSOC 联动：支持与 NGSOC 联动，防火墙支持发送日志 NGSOC，NGSOC 可以向防火墙下发处置策略，支持人工处置。

## 2.6 安全诊断功能

1. 在线抓包：支持在 Web、CLI 下的在线抓包。一条抓包工具可选择多个接口。

2. 检测工具：支持 ping 检测、端口检测、traceroute 检测；支持接口

Netflow 流量采集：连接监控器支持 HA 接口流量监控。

3. 调试工具：支持 CLI 下的调试工具。

4. 云端运维：支持防火墙运维文件通过云沙箱接口上传到云，提供云端运维支持。

### 3. 特点与优势

#### 3.2 三重云+五大联动

##### 三重云

木马云：木马云查杀功能，可以有效补充本地木马库不足，解决无法抵御未知木马问题。

病毒云：病毒云查杀功能，可第一时间拦截新病毒、未知病毒，并将病毒库扩充到 20 亿。

URL 云：URL 云查询功能，可极大扩充本地 URL 库，解决本地 URL 库分类少，资源不足问题。

##### 五大联动

情报威胁：防火墙可以接收来自奇安信安全云的威胁情报，根据情报生成动态策略，以此确认未知数据是正常数据还是恶意数据，并根据结果进行下一步的阻断或者放行处理。防范以多种形态出现的新恶意软件和 DDoS 攻击，以及 APT、0-day 等攻击所带来的日益增长的威胁。

终端协同：通过与天擎终端安全管理平台联动，防火墙可以实现应用识别的增强，更加精准的完成对应用的限流、阻断、过滤功能。

天眼、蜜罐联动：支持与天眼系统联动。防火墙支持发送常用协议头部信息给天眼。支持加密传输方式。天眼可以向防火墙下发域名、URL、恶意 IP 等处置策略。

NGSOC 联动：防火墙支持发送日志 NGSOC。NGSOC 可以向防火墙下发处置策略。支持人工处置。

沙箱联动：进行文件静态检测和动态检测，从而可以识别出未知威胁文件。

### 3.3 安全隔离的虚拟系统

虚拟系统功能可以将网神 SecGate 3600 防火墙系列虚拟成多个相互隔离并独立运行的虚拟系统，每一个虚拟系统都可以为用户提供定制化的安全防护功能，并可配备独立的管理员账号。在用户网络不断扩展时，通过虚拟系统功能不仅能有效降低用户网络的复杂度，还能提高网络的灵活性。当这些相互隔离并独立运行的虚拟防火墙系统需要通讯时，可以通过网神 SecGate 3600 防火墙系列提供的虚拟接口实现，而不需要通过物理链路将它们进行连接。

### 3.4 智能动态策略快速拦截攻击

网神 SecGate 3600 防火墙系列配备智能动态策略机制，当入侵防护、木马专项防护、防弱口令扫描等模块对异常流量进行过滤识别后，防火墙会提取攻击特征并生成智能动态策略，当攻击持续不断流入防火墙时，攻击特征被记录的异常流量会直接命中动态策略，快速拦截在防火墙之外。在目前攻击手法越来越偏向混合攻击+大流量攻击组合进攻的当下，智能动态策略可以为防火墙节省大量资源用来应对大流量混合攻击，并保证正常数据的通过。

### 3.5 应用层综合安全防护技术

网神 SecGate 3600 防火墙系列不仅提供多达 23 种普遍的基于网络层的攻击防护，并配备入侵防护、病毒检测、地址黑白名单、域名黑白名单功能。针对 HTTP、DNS、DHCP 协议提供针对性、多级别、适用于不同场景的应用层安全防护，更提供木马专项查杀、防弱口令扫描、局域网多播广播防护等功能，覆盖用户内外网安全。

### 3.6 完善的内网 DLP（数据防泄漏）

网神 SecGate 3600 防火墙系列具有邮件过滤，文件过滤，内容过滤功能，其中邮件过滤支持基于 RBL 黑名单以及自定义本地黑白名单的邮件过滤、同时能够基于收发件人关键字进行邮件过滤；文件过滤支持针对 HTTP、SMTP、POP3、

IMAP、FTP 协议传输的文件进行过滤，主要包含 3 大类：文档类、压缩类、归档类；内容过滤支持针对 HTTP、SMTP、POP3、IMAP、FTP 协议内容进行过滤，支持预定义关键字，包含身份证号、手机号等 5 类，支持基于内容过滤的页面推送功能，支持自定义添加关键字，可以正则匹配或者完全匹配。

## 4. 客户价值

### 4.1 智慧防御：全面防护网络攻击

通过威胁情报、安全大数据和协同联动等新技术的运用，极大消除传统防御盲区，有效防御并预防病毒、漏洞利用、恶意软件、僵尸网络等主流威胁由网络边界侵入，进而实现全面、高效的业务网络防护。

### 4.2 智慧感知：及时洞察潜在威胁

基于精准的高级威胁发现能力和配套的可视化工具、平台运用，显著增强网络的全局可见性和网络威胁的感知能力，通过实时洞察威胁态势、防御漏洞和失陷资产，及时发现网内潜伏的异常风险及高级威胁。

### 4.3 智慧管理：提升响应处置效率

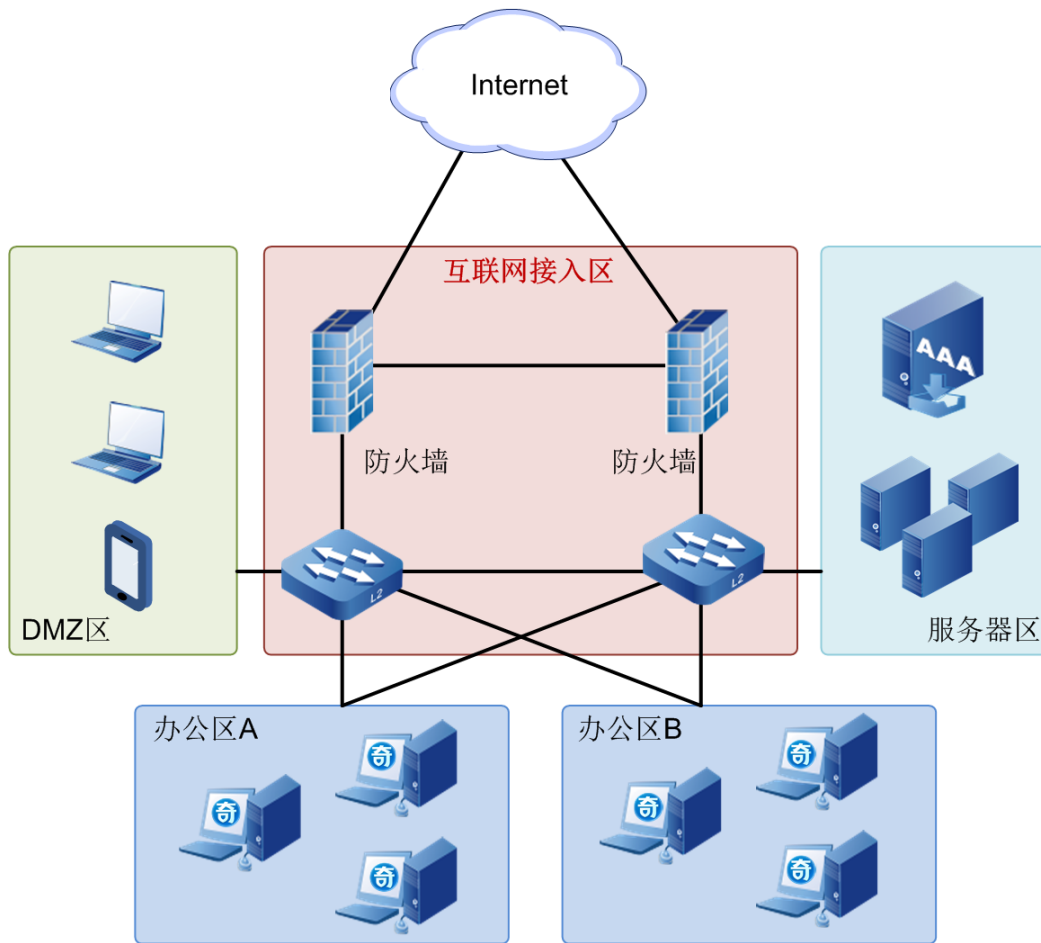
基于智能化的人机协同设计及配套的管理分析平台，持续助推用户的安全运营落地，大幅降低规模化部署用户的运维管理成本，避免误配置风险，并显著提升快速响应和处置的能力。

## 5. 应用场景

### 5.1 企业互联网边界安全应用场景

**客户痛点：**外部威胁多，上网用户网络安全意识参差有别；内部网络流量成分复杂；重点业务保证，需对上网的带宽及行为进行约束。

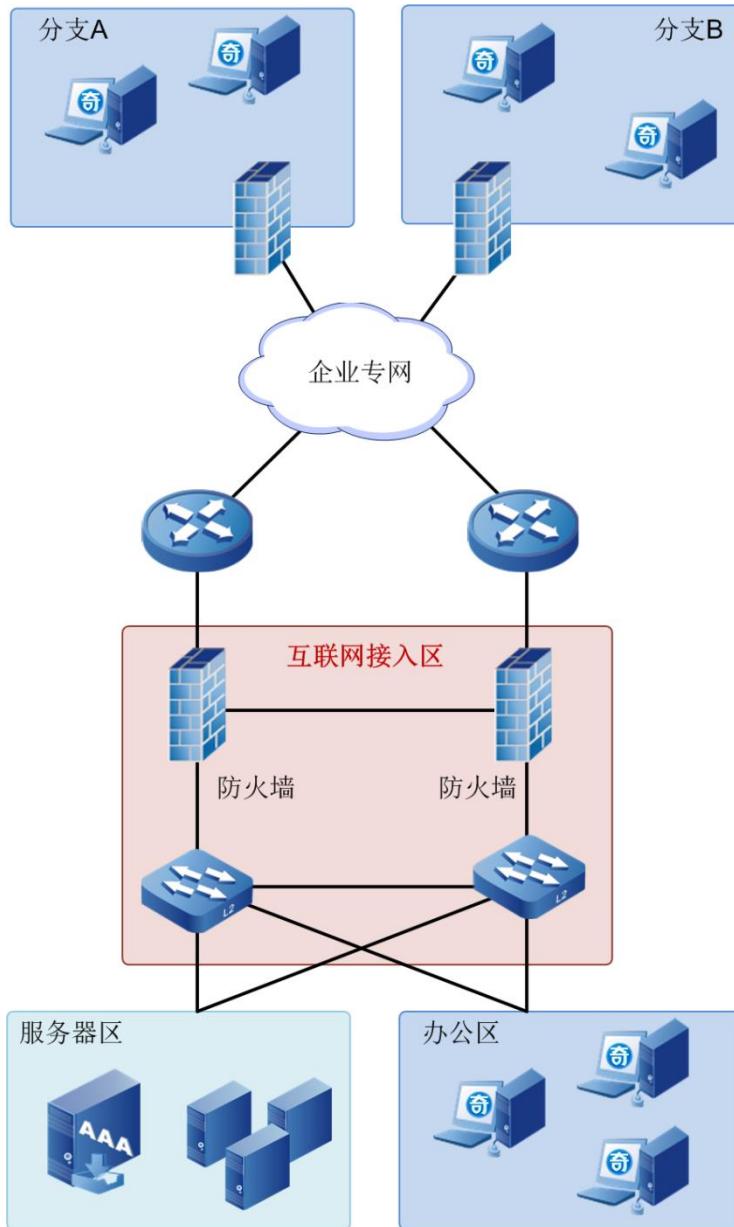
**优势：**与终端关系系统联动，实现对用户终端的统一管理，按照安全风险进行精细化管控、与 NAC 一起实现网络准入和访问控制；全面健壮的应用层级综合安全防护；按需动态调整带宽



## 5.2 行业专网网络安全应用场景

**客户痛点：**多链路备份，提升网络可用性；多分支互联，业务安全传输；重点业务保证，需对上网的带宽及行为进行约束；内部网络流量成分复杂；外部威胁多，上网用户网络安全意识参差不齐。

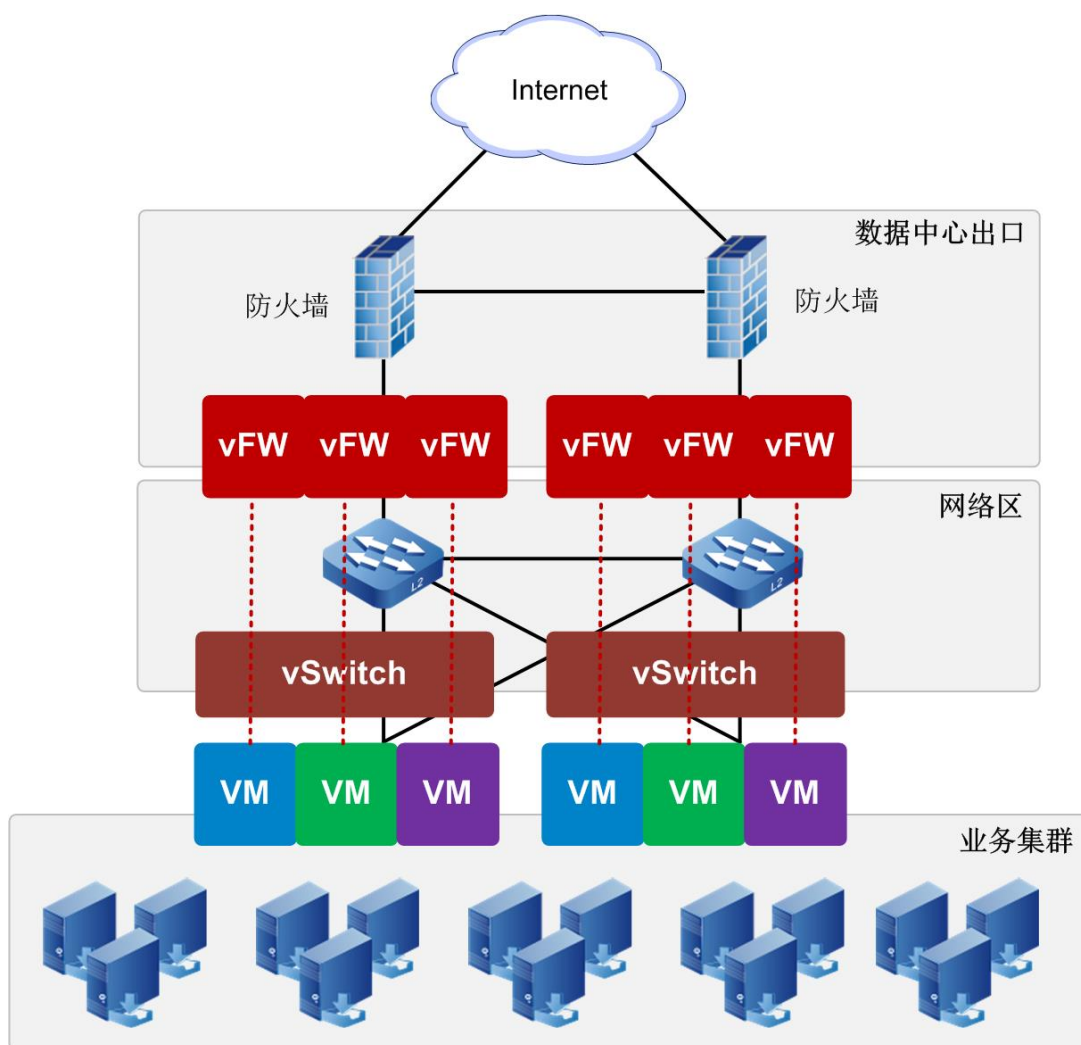
**优势：**高效的双机热备；标准的 IPsec VPN、SSL VPN 功能；按需动态调整带宽；全面健壮的应用层级综合安全防护；与终端联动，增强对木马及应用程序的精准识别、对用户终端按照安全风险进行精细化管控、与 NAC 一起实现网络准入和访问控制。



### 5.3 数据中心出口安全应用场景

**客户痛点：**出口大流量承载；全网可靠性要求高；全网安全性要求高；业务众多且网络复杂度高；需对业务实现安全隔离与管理。

**优势：**高性能承载出口大流量；全网冗余设计保证可靠性；5000+漏洞利用防护、间谍软件双向检测、实时检测已失陷服务器；虚拟防火墙承载业务实现安全隔离；独立配置、独立分析、独立维护。



## 5.4 多分支企业组网安全应用场景

**客户痛点：**多分支互联，业务安全传输；总部/分支一体化防御策略，对外部访问的安全控制；终端安全性保证，防止单台终端被突破导致的全网风险；多台防火墙统一管理、状态监控和数据分析

**优势：**出口部署智慧防火墙，分支机构与总部建立VPN，实现链路互为备份及负载，并实现边界安全隔离及互联网威胁攻击防御；对全网流量进行深度威胁检测，并利用本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警、阻断高隐蔽性威胁；与天擎协同联动，实现网关与本地的双重病毒查杀，以及基于终端风险的访问控制；部署SMAC系统，构建集配置批量下发、状态统一监控、失陷主机预警于一体的集中管理分析平台

