奇安信
新 一 代 网 络 安 全 领 军 者

可控安全
Controllable
Security

网神 SecGate3600 防火墙

技术白皮书

文档版本 01

奇安信集团
https://www.qianxin.com

奇安信集团为客户提供全方位的技术支持和服务。直接向奇安信购买产品的用户，如果在使用过程中有任何问题，可与公司总部联系。

读者如有任何关于本产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

网址：　　www.qianxin.com

技术支持热线：95015

地址：　北京市朝阳区来广营创远路 36 号院朝来高科技产业园 7 号楼

版权声明

Copyright © 2006-2021 奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

免责说明

奇安信集团，是专注于为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务的网络安全公司，包括但不限于以下主体：**奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司**，以及上述主体直接或者间接控制的法律实体。奇安信集团在此特别声明，对如下事宜不承担任何法律责任：

1. 本产品经过详细的测试，但不能保证与所有的软硬件系统或产品完全兼容，不能保证本产品完全没有错误。如果出现不兼容或错误的情况，用户可拨打技术支持电话将情况报告奇安信集团，获得技术支持。
2. 在适用法律允许的最大范围内，对因使用或不能使用本产品所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、贸易中断、商业信息的丢失或任何其它经济损失，奇安信集团不承担任何责任。
3. 对于因电信系统或互联网网络故障、计算机故障或病毒、信息损坏或丢失、计算机系统问题或其它任何不可抗力原因而产生的损失，奇安信集团不承担任何责任，但将尽力减少因此而给用户造成的损失和影响。
4. 对于用户违反本协议规定，给奇安信集团造成损害的，奇安信集团将有权采取包括但不限于中断使用许可、停止提供服务、限制使用、法律追究等措施。
5. 对于从非奇安信集团指定站点下载的本产品以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证该产品是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件，使用此类软件，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。
6. 无论在任何原因下（包括但不限于疏忽原因），对任何人通过使用本产品上的信息或由本产品链接的信息，或其他与本产品链接的网站信息所导致的损失或损害（包括直接、间接、特别或后果性的损失或损害，如收入或利润之损失，电脑系统之损坏或数据丢失等后果），奇安信集团不承担任何由此产生的一切法律责任。

以上声明最终解释权归奇安信集团所有。

文档说明

文档名称	网神 SecGate3600 防火墙 技术白皮书		
产品版本	V3.6.6.0（-8.1.13.104327&8.11.13.104327&6.90.13.104327&6.91.13.104327）		
扩散范围	产品经理/售前/售后	**文档版本号**	01
作者	佟宇霆	**日期**	2020-09-27
初审人	孙广伟	**复审人**	曹红军
修订记录	2020-10-21：文档第一次发布。		

目 录

1 产品概述.....1

2 产品特色.....2

2.1 产品形态及架构.....2
2.2 灵活的管理接口.....4
2.3 管理员权限分权分立.....4
2.4 安全隔离的虚拟系统.....5
2.4.1 概述.....5
2.4.2 一机多用，节省投资.....5
2.4.3 灵活配置，方便管理.....6
2.4.4 业务隔离，互不影响.....6
2.5 IPv6 Ready.....6
2.5.1 IPv4/IPv6 双栈.....6
2.5.2 跨栈隧道方案.....7
2.6 多层次可靠性保证，整机可靠性高.....10
2.6.1 硬件可靠性.....10
2.6.2 整机可靠性.....13
2.6.3 系统可靠性.....19
2.6.4 链路可靠性.....19
2.7 全面、智能的路由功能.....24
2.7.1 全面的路由功能.....24
2.7.2 精确的多出口 ISP 路由智能选路.....24
2.7.3 对称路由保证来回路径一致.....25
2.7.4 高适应性的路由负载均衡算法.....25
2.8 全面的 SSL 解密防护.....25
2.8.1 SSL 解密.....25
2.8.2 SSL 入站检查.....26
2.9 丰富的 VPN 隧道类型.....26
2.10 强大的识别功能，实现精细化管控.....26
2.10.1 用户识别.....26

2.10.2 服务识别.....28
2.10.3 应用识别.....28
2.10.4 内容识别.....29
2.10.5 URL 识别.....30
2.10.6 行为识别.....30
2.10.7 地理位置识别.....31
2.10.8 精细化的安全策略.....31
2.11 深度安全检测及 DLP，保护网络安全.....32
2.11.1 概述.....32
2.11.2 全面的应用层攻击防护能力.....33
2.11.3 先进的多维动态特征异常检测引擎.....34
2.11.4 灵活的自定义漏洞/间谍软件特征功能.....35
2.11.5 多维度的 DLP 数据防泄漏.....35
2.11.6 强大的威胁情报渗透.....35
2.12 多系统联动防护，构建立体式防护体系.....36
2.12.1 防火墙和终端系统联动.....37
2.12.2 防火墙和天眼系统联动.....37
2.12.3 防火墙和 NGSOC 系统联动.....37
2.12.4 防火墙和天御云系统联动.....38
2.12.5 防火墙和 ITS 系统联动.....38
2.12.6 防火墙和蜜罐联动.....41
2.13 应用及流量可视化，网络行为无所遁形.....43
2.13.1 概述.....43
2.13.2 大容量、多维度日志.....43
2.13.3 多样化的日志检索方式.....44
2.13.4 全方位风险信息展示及分析.....44
2.13.5 强大的内容审计策略.....44
2.14 自动化应急响应功能.....44
3 技术优势.....46
3.1 采用第四代 SecOS 系统.....46
3.2 整体框架采用 AMP+并行处理架构.....46
3.3 优化的 AMP+架构突破传统 SMP 架构瓶颈.....47
3.4 更优化的网口数据收发处理.....49
3.5 单引擎一次性数据处理技术.....50
3.6 多级冗余架构提高防火墙可靠性.....51
3.7 云端协同扩展精确定位威胁.....52
3.8 基于 NDR 安全体系的未知威胁闭环防御.....52
4 应用场景.....54
4.1 企业互联网边界安全应用场景.....54

4.1.1 典型场景.....54
4.1.2 痛点和优势.....55
4.2 行业专网网络安全应用场景.....56
4.2.1 典型场景.....56
4.2.2 痛点和优势.....57
4.3 数据中心出口安全应用场景.....58
4.3.1 典型场景.....58
4.3.2 痛点和优势.....58
4.4 多分支企业组网安全应用场景.....60
4.4.1 典型场景.....60
4.4.2 痛点和优势.....61

1 产品概述

随着信息化的飞速发展，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。传统的安全设备存在以下问题：

1. 以本地规则库为核心，无法有效检测已知威胁。
2. 没有数据智能，无法感知未知威胁。
3. 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，传统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。

网神 SecGate3600 防火墙（以下简称为：防火墙）是奇安信集团自主创新的新一代防火墙安全系统，基于 NDR（基于网络的检测与响应）安全体系，在高性能和先进架构的支撑下，集成了防火墙、VPN、应用与身份识别、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能，并支持与天眼、终端管理系统、NGSOC、天御云等多系统进行协同防御。

在扩展了协同防御能力的基础上，在防火墙上以分析中心、数据中心、处置中心三大中心为核心，实现了对威胁的分析、定位、处置一体化过程。是专门为政府、军队、金融、教育、运营商、企业的网络出口打造的基于协同防御体系的新一代网络安全防御系统。

2 产品特色

2.1 产品形态及架构

产品名称	网神 SecGate 3600 防火墙系统 v3.6.6.0	
产品型号	NSG6000-TX15	
商品编码	NSG6000-TX15P-QW	NSG6000-TX15M-QW
内存	16G	
硬盘	默认 1T HD 硬盘，可选（128G SSD、4T HD 硬盘）	
网络层吞吐（bps）	30G	
标配并发连接数	≥600 万	
应用层吞吐量（bps）	20G	
每秒新建连接数（CPS）	30 万	
标配 SSL VPN 在线用户数	32	
最大 SSL VPN 在线用户数	300	
标配 IPsec VPN 隧道数	32	
最大 IPsec VPN 隧道数	5000	
标配 PPTP VPN 隧道数	50	
标配 L2TP VPN 隧道数	50	
MTBF（小时）	100,000	

延时	27 μs	
板载电口 10/100/1000Base-T 个数	16	
板载 SFP 千兆光口插槽个数	6	
板载 SFP+万兆光口插槽个数	8	
扩展槽个数	2	
异步串行管理接口	1	
HA 接口	1	
管理口	1	
USB 接口(3.0)	2	
机箱规格&尺寸	1U 深 560mm*宽 440mm*高 44mm	1U 深 560mm*宽 440mm*高 44mm
机架规格	19 寸	
温度和湿度	工作温度:0~40℃，存储温度:-25~70℃，相对湿度：5~90%不凝结	
电源	单电源，输入电压，冗余风扇：100-240VAC，最大输出功率：250W	冗余电源，输入电压，冗余风扇：100-240VAC，最大输出功率：250W
可选模块	NSG6000-TX-4TP-QW NSG6000-TX-8TP-QW NSG6000-TX-4SP-MM-QW NSG6000-TX-4SP-SM-QW NSG6000-TX-4XP-MM-QW NSG6000-TX-4XP-SM-QW SFP 模块/VPN 模块 IPS/APP/AV/URL/IOC	

2.2 灵活的管理接口

防火墙支持通过业务接口或 MGT 管理接口进行设备管理，适用于不同的用户环境。

管理方式	特点
业务接口	无需搭建额外的、专用的管理网络，减少了网络复杂度和额外的网络维护开支。 支持配置接口下的管理方式（HTTP、HTTPS、Ping、SSH、SNMP）和可信管理主机，最大程度上减少管理风险。
MGT 管理接口	管理平面与业务平面分离，在业务数据量较大的情况下，也不会影响对防火墙的正常管理。 独立的管理接口可以严格限制管理防火墙的终端，保证防火墙的管理安全。 支持配置接口下的管理方式（HTTP、HTTPS、Ping、SSH、SNMP）和可信管理主机，最大程度上减少管理风险。

2.3 管理员权限分权分立

防火墙支持基于管理员的角色的分权分立管理员帐号机制，支持三权分立功能，根据用户的操作场景需求：

- 系统预定义了超级管理员、安全管理员、系统管理员、审计管理员、RESTful API 管理员和 OpenC2 联动管理员。实现配置管理、安全管理、审计管理、RESTful API 和联动功能分离的同时，也保证了管理员权限的隔离。
- 防火墙支持自定义管理员角色，每种角色可以细粒度地指定系统功能模块的读写权限，方便用户管理系统。

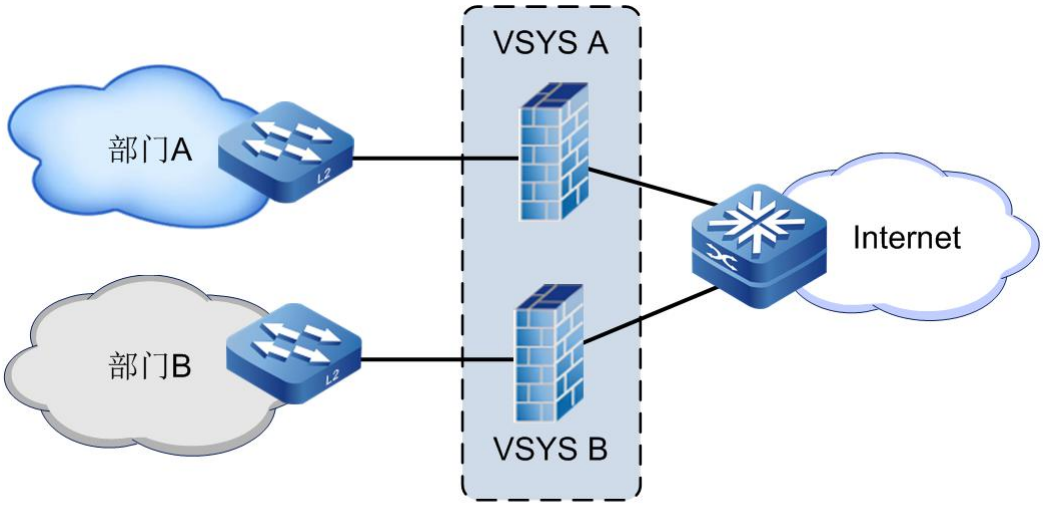
2.4 安全隔离的虚拟系统

2.4.1 概述

防火墙支持虚拟系统功能，将防火墙虚拟成多个相互隔离并独立运行的虚拟防火墙，并支持进行系统资源划分。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，可以通过防火墙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。

图 2-1 虚拟防火墙部署组网



2.4.2 一机多用，节省投资

在传统防火墙部署方案中，业务服务器与防火墙基本上是 1:1 配比。因此，当业务增加时，用户需要购置新的防火墙。然而当业务减少时，对应的防火墙就闲置下来，导致投资浪费。

虚拟防火墙技术以其灵活可扩展的特性帮助用户保护投资，用户可以随时根据业务增减相应的虚拟防火墙。

2.4.3 灵活配置，方便管理

虚拟防火墙技术允许数据中心根据客户的性能需求，量身定做不同性能指标的虚拟防火墙。例如，可以向某些客户出租 10M 吞吐量的虚拟防火墙，而向另一些客户出租 100M 吞吐量的虚拟防火墙。

2.4.4 业务隔离，互不影响

业务类型多种多样，需要使用的防火墙安全策略也不同。例如，DNS 服务器需要进行 DNS Query Flood 攻击防护，而 HTTP 服务器则需要进行 HTTP Get Flood 攻击防护。虚拟防火墙的划分能够实现不同业务的专属防护策略配置。

同时，CPU 资源虚拟化支持隔离虚拟防火墙之间的故障和性能瓶颈，当单个虚拟防火墙受到攻击或资源耗尽时，其它虚拟防火墙不会受到影响，极大地提升了各业务的综合可用性。

2.5 IPv6 Ready

2.5.1 IPv4/IPv6 双栈

防火墙支持完整的双栈协议，支持 IPv6 下的多种功能，包括网络功能和安全功能，从用户的角度看，其就像支持两个并发的网络。

功能指标项	功能描述
IPv6 接口	支持接口 IPv6 地址配置
	支持使用 IPv6 地址进行设备管理
	支持 IPv6 手动及自动的 IP/MAC 探测及绑定
	支持 SLAAC 功能
	支持发布 RA
IPv6 路由	支持 IPv6 下静态路由、策略路由、动态路由（RIPng、OSPFv3、BGP4+）
	支持 IPv6 邻居的动态管理和静态配置
IPv6 认证管理	支持 IPv6 的本地认证
	支持 IPv6 Web 认证
IPv6 日志管理	支持 IPv6 的 SYSLOG、SNMP

功能指标项	功能描述
IPv6 VPN	支持 IPv6 跨栈隧道技术（6to4、ISATAP、手工隧道）
	支持 DS-Lite 功能，支持 B4 和 AFTR 组网角色。
DHCPv6	支持 DHCPv6 Server
	支持 DHCPv6 Relay
DNS	支持静态 DNS
	支持基于入接口、源地址或目的地址选择 DNS 代理服务器
	支持基于出接口选择 DNS 代理服务器
NAT	支持 NAT-PT，支持 4to6、6to4 的 SNAT 和 DNAT 以及双向地址转换进行地址映射
	支持 NAT64 和 DNS64
	支持 NAT66，支持一对一、多对一、多对多和 NPTv6（ALG 仅支持 FTP 和 TFTP）
	支持静态路由、OSPF 等三层网络协议
IPv6 安全功能	基于 IPv6 的漏洞防护、防间谍软件、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控等安全功能
	支持 IPv6 扩展头安全性检测，支持 MAC 一致性检查
	支持 NDP 防护，支持基于 IPv6 的异常包防护、ICMPv6 管控
	支持配置基于 IPv6 的安全策略、SSL 解密策略
	支持基于 IPv6 的会话限制及会话统计
	支持基于 IPv6 的数据中心和分析中心
网络功能	支持配置源地址路由、源接口路由、目的接口路由、目的地址路由

得益于完全自主研发的 AMP+架构与第四代 SecOS 操作系统的支撑，防火墙系统在 IPv6 性能上可以媲美 IPv4 性能。

2.5.2 跨栈隧道方案

防火墙支持多种跨栈隧道解决方案，方便用户在 IPv6 演进过程中的跨栈报文传输需求。主要包括：

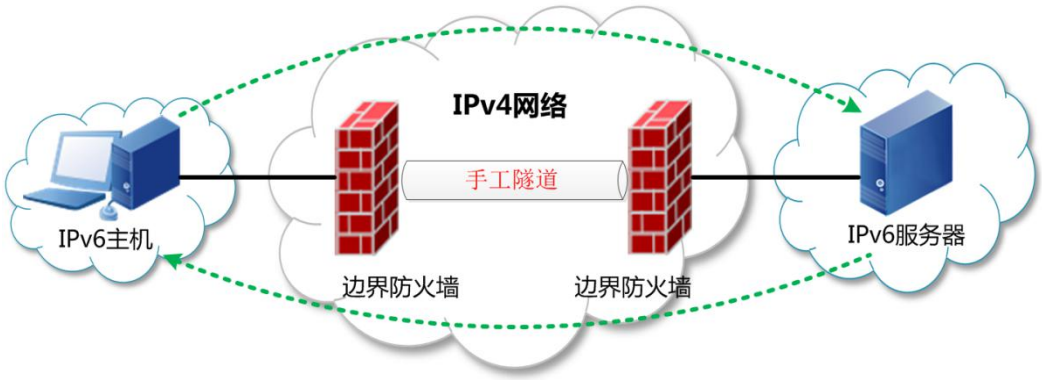
- 6in4 跨栈隧道方案
- GRE 跨栈隧道方案
- NAT64/DNS64 方案

6in4 跨栈隧道方案

防火墙支持 6in4 跨栈隧道。允许 IPv6 主机穿越 IPv4 网络访问到另一台 IPv6 主机或者 IPv6 服务。

防火墙支持三种 6in4 隧道，分别为手工隧道、ISATAP、6to4 隧道。

图 2-2 手工隧道典型应用场景举例

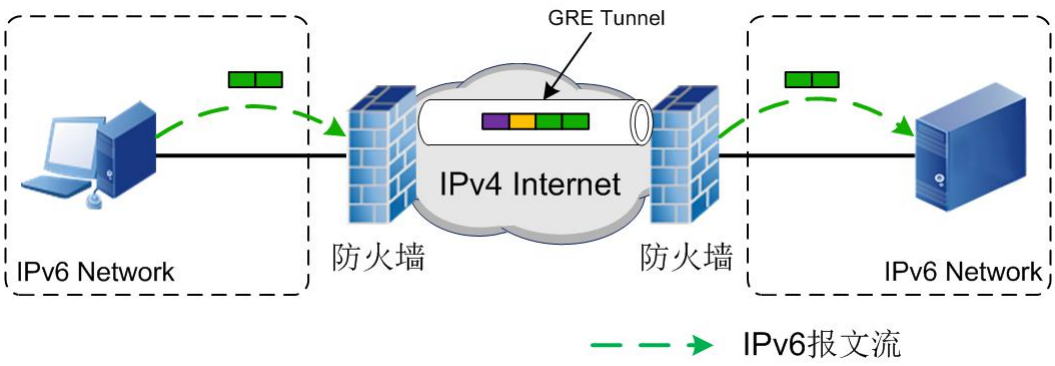


GRE 跨栈隧道方案

GRE（Generic Routing Encapsulation，通用路由封装协议）提供了将一种协议的报文封装在另一种协议报文中的机制，使 IPv6 报文能够通过隧道封装，在 IPv4 网络传输。

GRE 隧道可以将 IPv6 报文作为净荷，在外部增加 GRE 报文头和 IPv4 报文头后，在 IPv4 网络中传输。

图 2-3 GRE 跨栈隧道典型应用场景



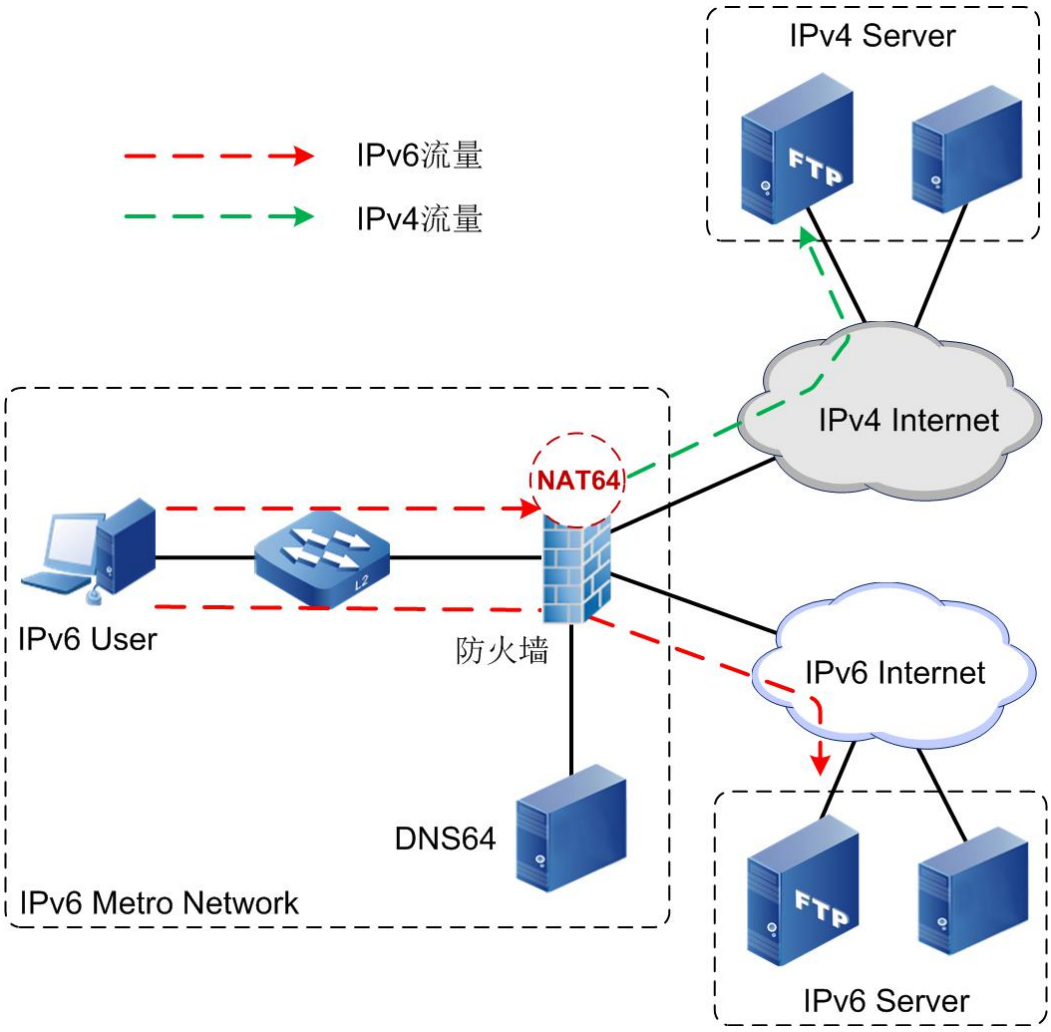
NAT64/DNS64 方案

在 IPv6 演进过程中，网络侧的 IPv6 Ready 程度较高，但是业务侧 IPv6 化还不乐观，有很大一部分资源仍然采用的是 IPv4 的地址。NAT64 技术就是为了解决 IPv6 终端访问 IPv4 资源时，地址从 IPv6 地址向 IPv4 转换的问题。

如图 2-4 所示。在防火墙上应用 NAT64 功能后，IPv6 用户访问 Internet 时的不同情况为：

- 如果目的 IP 地址为 IPv6 地址，则防火墙直接将报文转发到对应的 IPv6 网络中。
- 如果目的 IP 地址为 IPv4 地址，则防火墙将报文中的 IPv6 地址转换为 IPv4 地址，再转发到对应的 IPv4 网络中。

图 2-4 NAT64 应用组网示意图

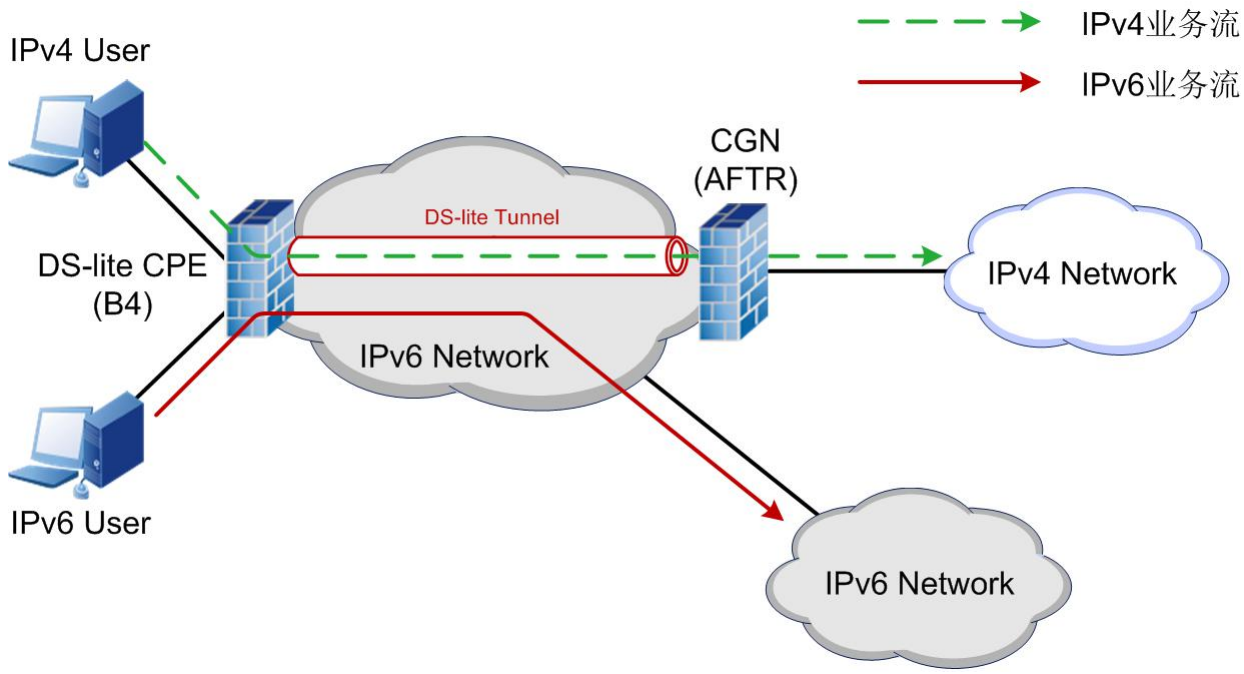


DS-Lite 方案

防火墙支持 DS-Lite 轻量级跨栈隧道方案，支持 B4 和 AFTR 组网角色。

通过隧道承载了 IPv4 流量在 IPv6 网络中进行传输，使得 IPv6 网络两端的终端无需支持 IPv4/IPv6 双栈协议，保证了其“轻量化”。典型组网如图 2-5 所示。

图 2-5 DS-lite 基本组网示意图



2.6 多层次可靠性保证，整机可靠性高

2.6.1 硬件可靠性

双冗余电源

防火墙部分型号支持冗余电源并支持电源模块的热插拔。

- 当系统同时使用两个电源模块时，两个电源模块共同进行负载分担。
- 当其中一个电源模块损坏或被拔出电源线时，另一个模块可以完全承担系统的负载，保证系统正确、稳定运行。
- 电源模块支持热插拔，用户可以在开机时，直接更换损坏的电源模块。

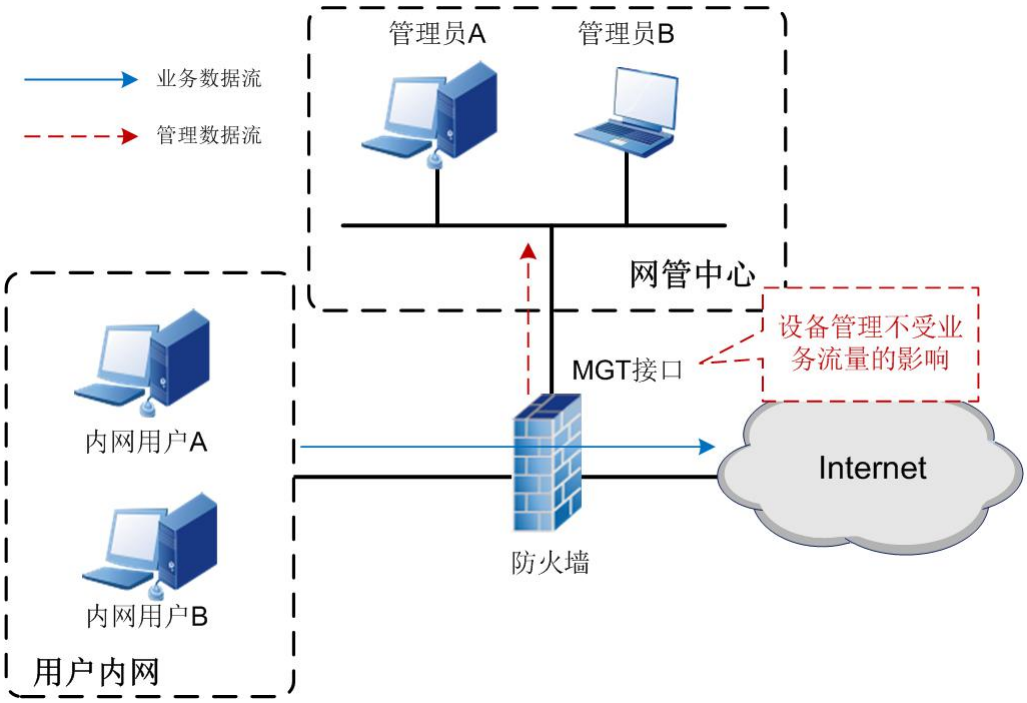


专用管理接口

防火墙支持通过 MGT 接口管理，支持利用专门搭建的管理网络完成设备管理，使得防火墙上管理数据和业务数据分离。使用 MGT 接口比使用业务接口能够提供更可靠的设备管理链路，在业务流量较大或者设备发生故障时，依然能够管理设备并定位故障信息。

带外网管示意图如图 2-6 所示。

图 2-6 带外网管示意图



硬件 Bypass 和看门狗

防火墙支持硬件 Bypass 和看门狗功能，防止由于系统故障导致网络不可用。

- 硬件 Bypass：当设备意外掉电时，通过防火墙的业务流可以直接通过防火墙，不会由于防火墙单点故障导致用户网络瘫痪。

- 硬件看门狗：当设备系统出错或宕机时，硬件看门狗会自动重启整个系统，防止由于防火墙以外宕机导致用户网络瘫痪。

说明

防火墙硬件 Bypass 功能由硬件接口板卡实现。

图 2-7 硬件 Bypass 原理示意图--正常状态

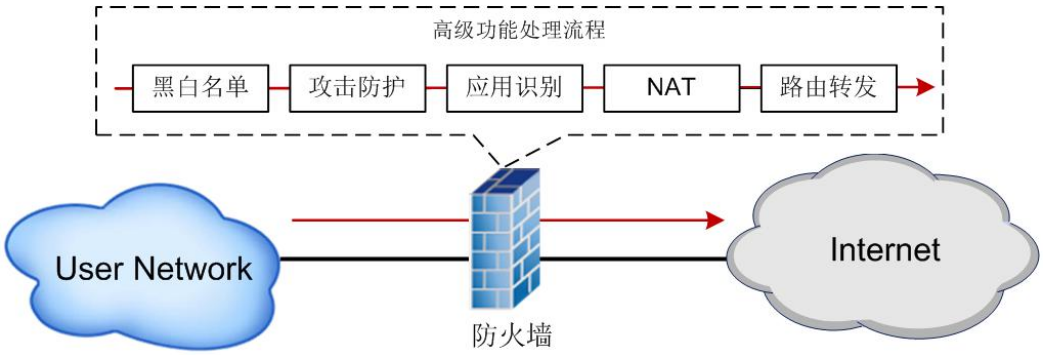
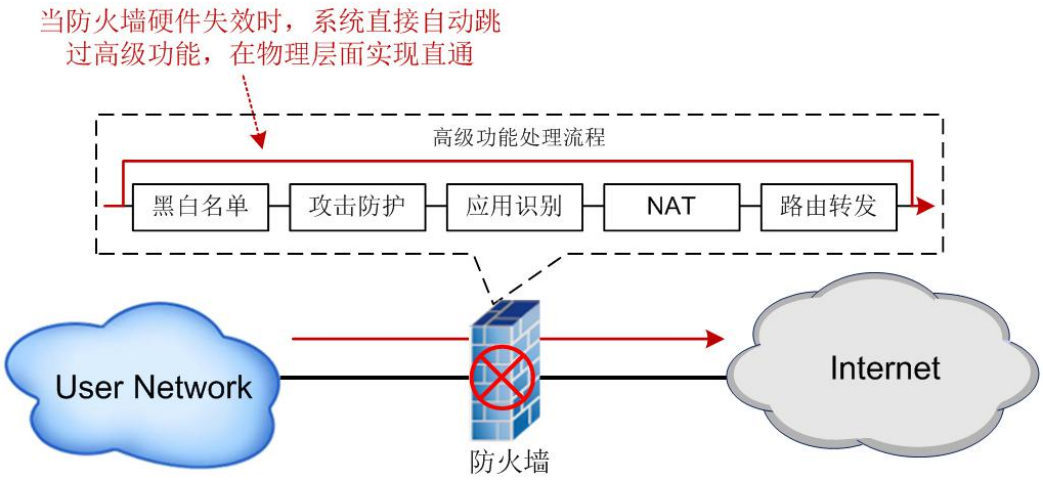


图 2-8 硬件 Bypass 原理示意图--硬件失效状态



ECC 内存

防火墙的中、高端型号使用了具备 ECC 技术的内存。能够保证系统长时间运行的稳定性。

ECC（Error Checking and Correcting，错误检查和纠正），是一种能够实现“错误检查和纠正”的技术。在内存中使用 ECC 技术，能够容许错误，并可

以将错误更正，使系统得以持续正常的操作，不致因错误而中断，保证系统的正常运行。

2.6.2 整机可靠性

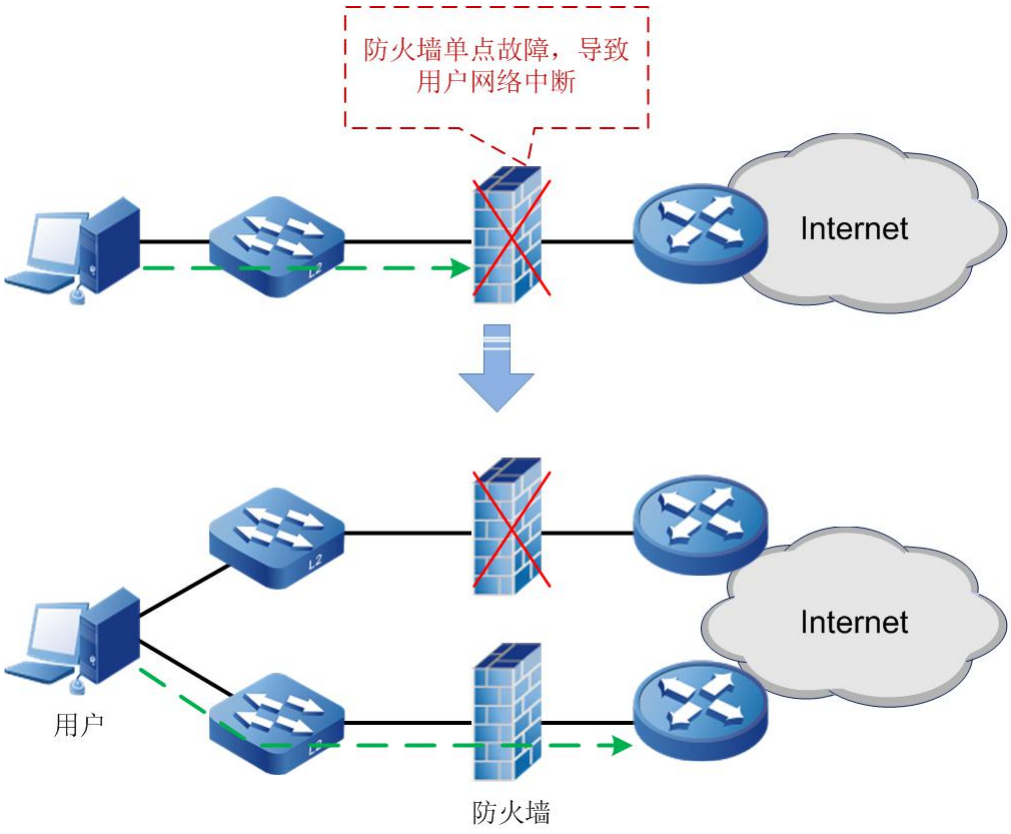
概述

防火墙系统支持多种灵活部署方式，提供不同场景下客户网络环境需求，支持路由模式、透明模式、虚拟网线模式、旁路镜像模式、主主、主备两种双机模式等多种部署方式。

单台防火墙部署在用户网络出口时，如果设备出现故障，就会造成链路中断，进而导致整个业务中断。

通过部署双机热备，在网络关键位置上部署两台防火墙，提高网络的可靠性。当一台设备故障时，可以通过另一台设备进行通信，保证业务正常运行。

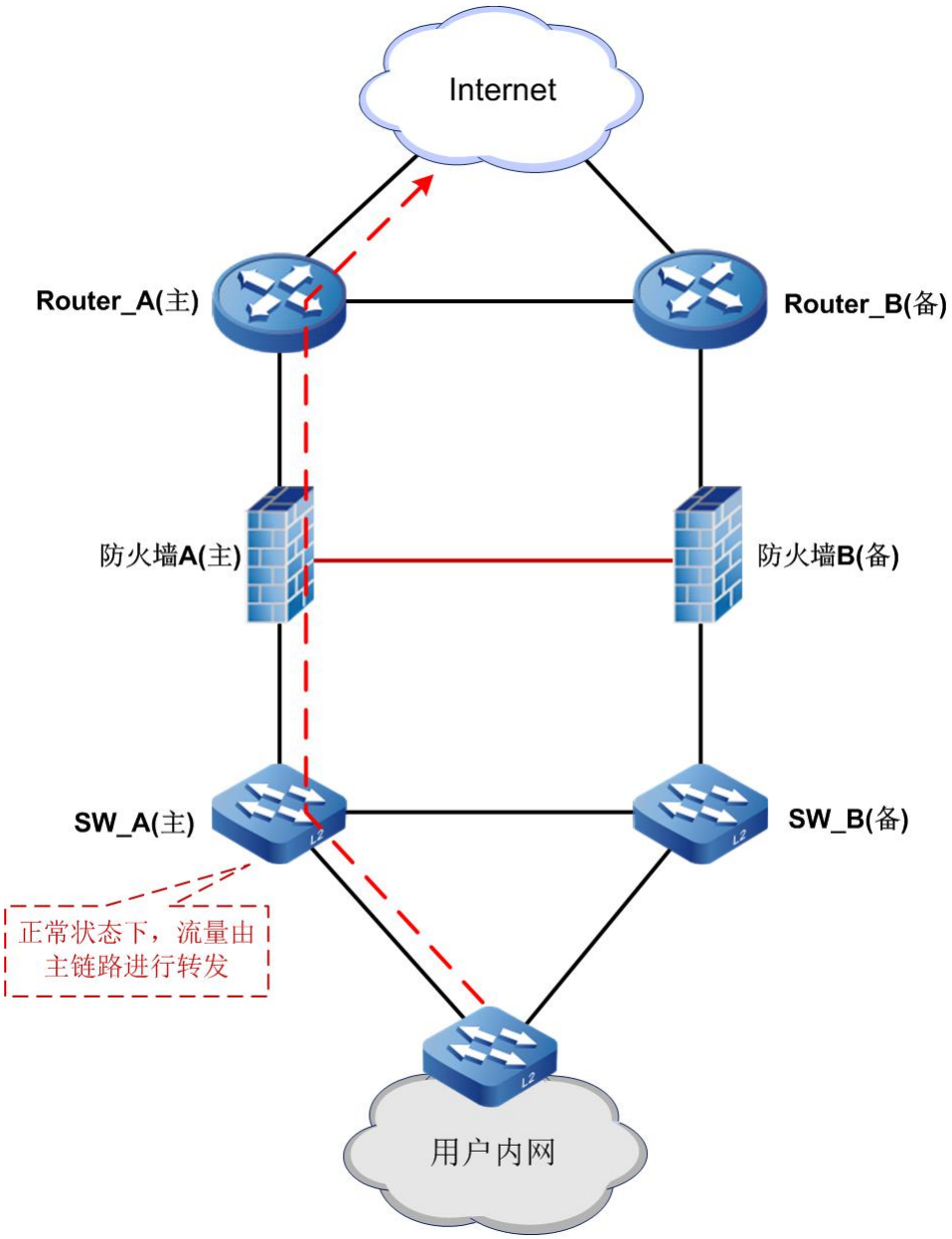
图 2-9 单点故障和双机热备



主备模式

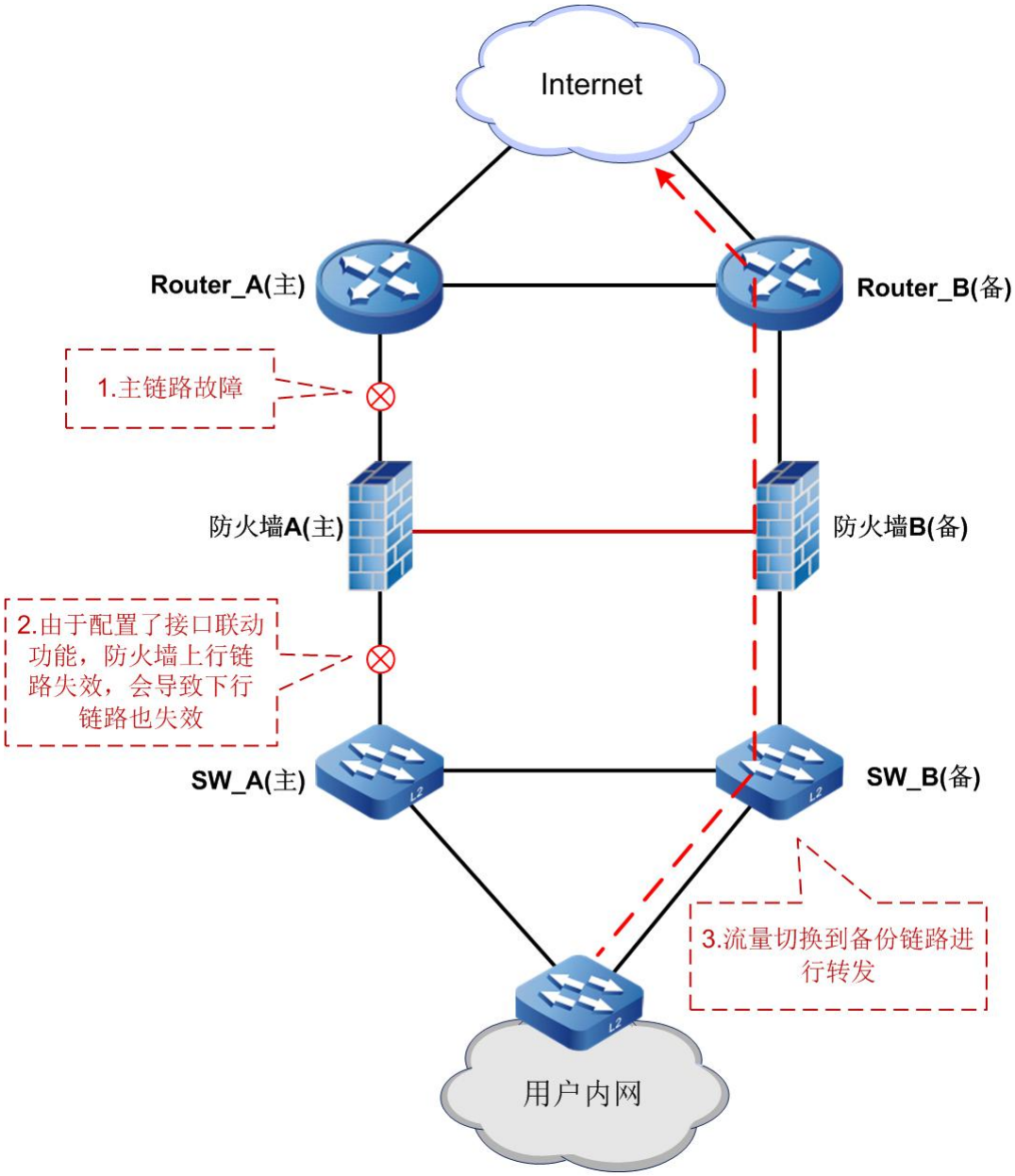
主备模式下，两台防火墙一台作为主设备，另一台作为备份设备。主设备负担所有报文转发工作，并将当前会话信息以及配置信息同步到备设备上。

图 2-10 主备备份（正常转发状态）



当主设备出现故障时，主设备自动变为备设备。原来的备设备转变为主设备，承担报文转发工作，可以实现无感知的网络切换。

图 2-11 主备备份（链路切换状态）

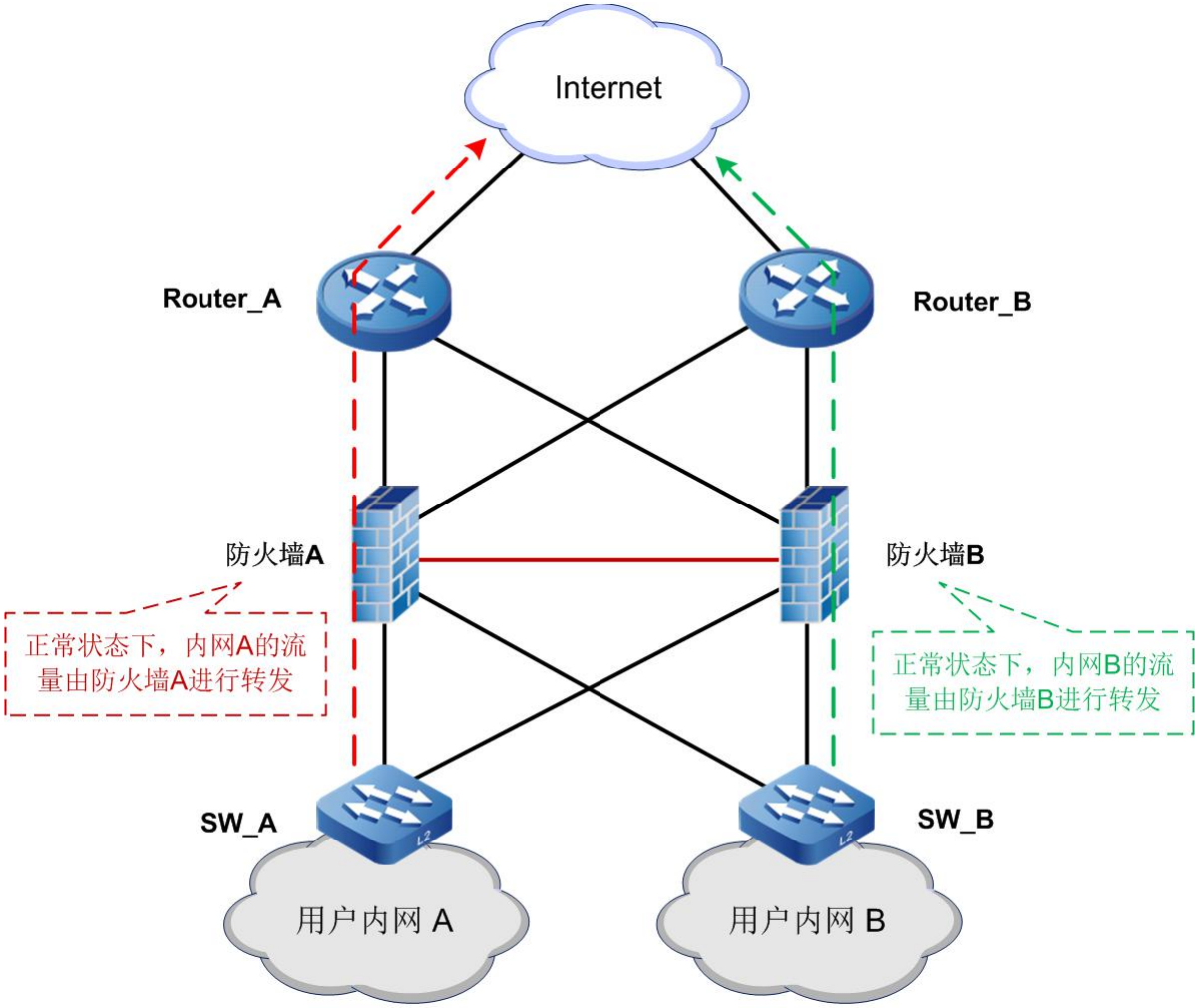


主主模式

主主模式下，防火墙分别配置两个 HA 组。

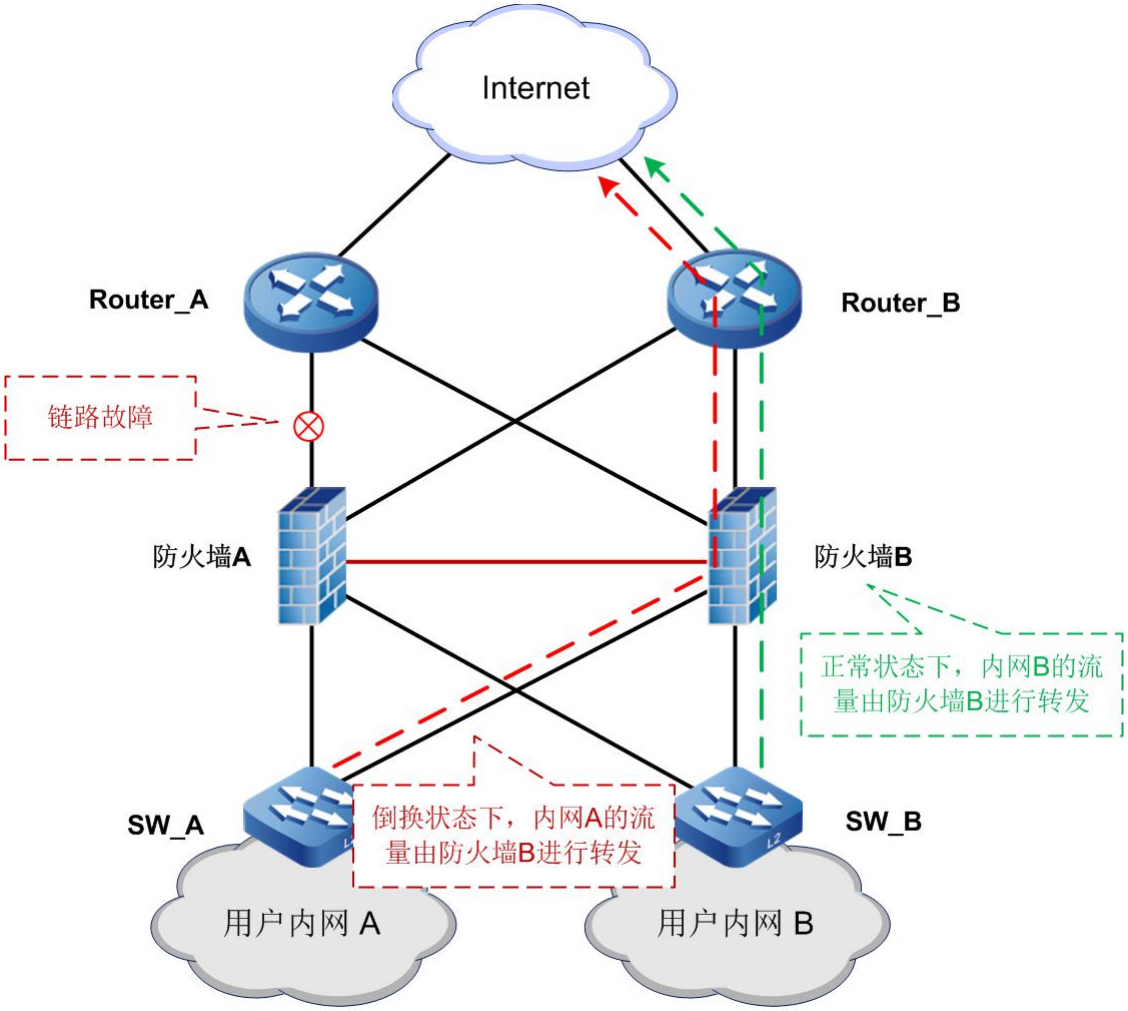
- HA 组 0：防火墙 A 为主设备，防火墙 B 为备份设备。正常状态下，User A 的流量由防火墙 A 转发。
- HA 组 1：防火墙 B 为主设备，防火墙 A 为备份设备。正常状态下，User B 的流量由防火墙 B 转发。

图 2-12 负载分担双机热备（正常转发状态）



当其中一台设备出现故障时，两个 HA 组的流量均切换到同一台设备，进行报文转发工作。

图 2-13 负载分担双机热备（链路切换状态）

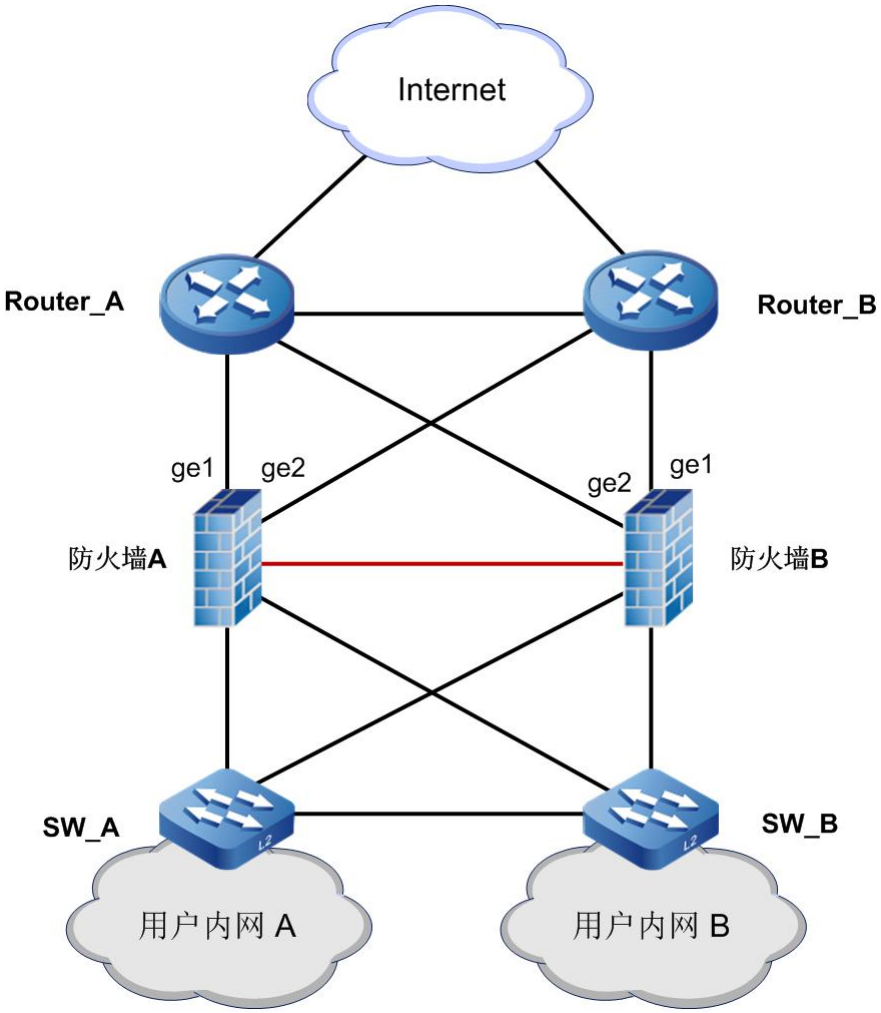


双机热备全冗余组网

在图 2-13 的基础上，将 SW_A 和 SW_B 相连，Router_A 和 Router_B 相连，这样就组成了双机热备的全冗余组网，如图 2-14 所示。

双机热备的全冗余组网能够进一步提升网络可靠性，避免多条链路故障时业务中断。例如，当防火墙 A 的 GE1、GE2 和防火墙 B 的 GE1 这三个接口都故障时，业务流量依然能够通过防火墙 B 的 GE2 接口转发。

图 2-14 双机热备全冗余组网



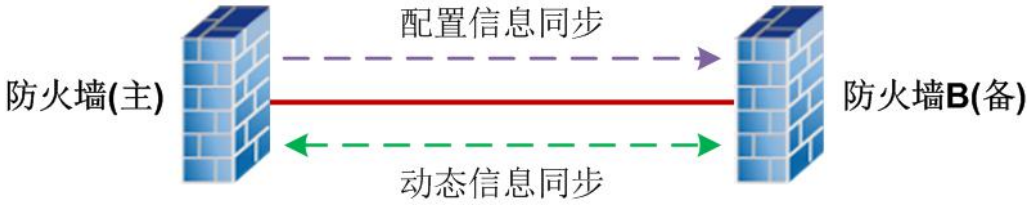
信息同步

如果是传统的网络设备（如路由器、三层交换机），只需要在两台设备上做好路由的备份就可以保证业务的可靠性，即当一台设备出现故障时，另一台设备能够接替故障设备处理业务，保证业务不中断。

而防火墙是状态检测设备，它会对一条流量的首包（第一个报文）进行完整的检测，并建立会话来记录报文的状态信息（包括报文的源 IP、源端口、目的 IP、目的端口、协议等）。而这条流量的后续报文只有匹配会话才能够通过防火墙并且完成报文转发，如果后续报文不能匹配会话则会被防火墙丢弃。因此，当防火墙双机部署时还需要考虑两台防火墙之间的会话等状态信息的备份。

- 配置信息同步：当主墙完成配置并使能 HA 功能后，配置信息会自动同步给备墙，使得备墙与主墙拥有完全相同的配置。配置信息为单向信息同步，仅从主墙同步给备墙。

- 动态信息通过：防火墙在进行数据转发时，会产生很多动态信息，例如会话信息，超时时间等。该类信息主墙和备墙可以实时互相同步，以保证主墙和备墙的动态信息一致。动态信息为双向信息通过，主墙和备墙可以互相同步。



2.6.3 系统可靠性

防火墙支持双系统备份：

- 当主系统出现故障时，可以切换到备份系统继续提供服务。
- 当系统升级失败时，可以使用备份系统启动防火墙，实现升级回退。
- 同时支持设备多虚一。

2.6.4 链路可靠性

手工静态链路聚合

防火墙支持手工静态方式的链路聚合。

手工聚合方式将多个物理端口加入 Trunk 组，形成一个逻辑端口，同一逻辑端口下的链路实现负荷分担，这种方式不利于观察链路聚合端口的状态。

802.3ad 方式链路聚合

符合 IEEE 802.3ad 协议的链路聚合方式，采用 LACP（Link Aggregation Control Protocol，链路聚合控制协议）协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）与对端交互信息。使能某接口的 LACP 协议后，该接口将通过发送 LACPDU 向对端通告自己的系统 LACP 协议优先级、系统 MAC、端口的 LACP 协议优先级、端口号和操作 Key。

对端接收到 LACPDU 后，将其中的信息与从其它接口所收到的信息进行比较，以选择能够处于 Selected 状态的端口，从而双方可以对端口处于 Selected 状态达成一致。操作 Key 是在链路聚合时，聚合控制根据端口的配置（即速率、双工模式、Up/Down 状态、基本配置等信息）自动生成的一个配置组合。在聚合组中，处于 Selected 状态的端口有相同的操作 Key。

防火墙支持 3 种不同的流量负载算法，如表 2-1 所示。

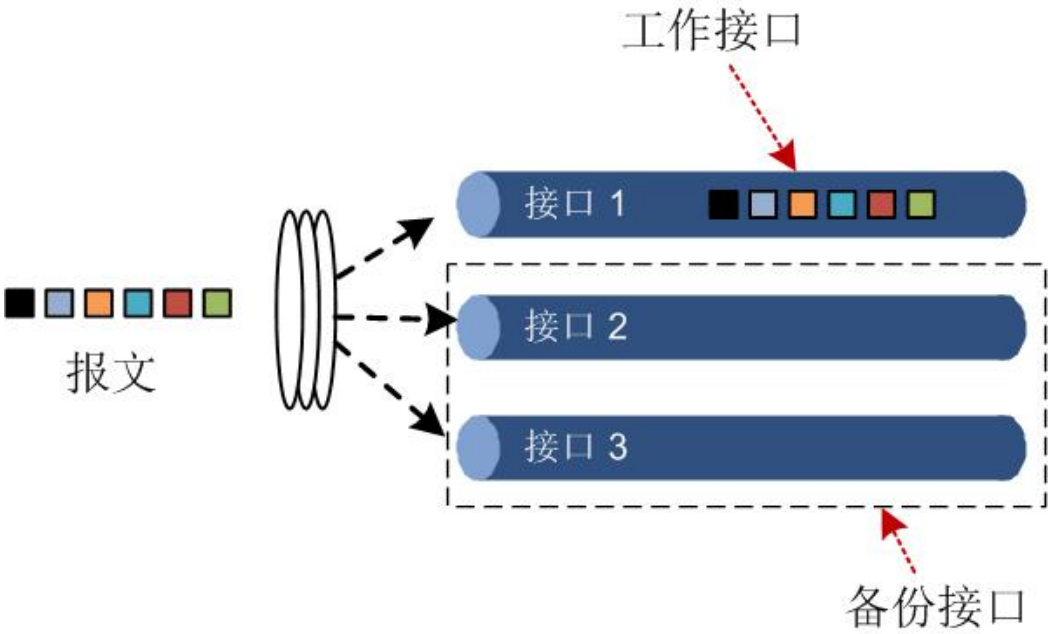
表 2-1 链路聚合流量负载算法

均衡负载算法	说明
根据 IP 地址和 TCP/UDP 端口组合均衡	使用 IP 地址和 TCP/UDP 端口进行哈希算法
根据源和目的 MAC 地址组合均衡	使用源和目的 MAC 进行哈希算法
根据 MAC 地址和 IP 地址组合均衡	根据 MAC 地址和 IP 地址进行哈希算法

热备方式链路聚合

热备方式，即聚合组所包含的接口为热备关系，一个为主，其余均为备。在正常工作时只有一个接口负责数据包收发，监测到故障时切换为备选接口当中的一个正常接口。如图 2-15 所示。

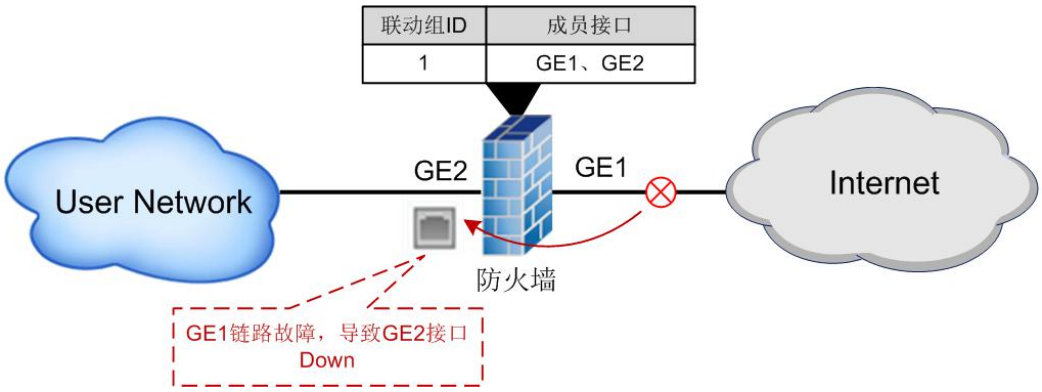
图 2-15 热备调度方式



接口联动

接口联动功能提供了一种接口联动方案，可以扩展链路备份的范围，即通过监控上行链路并对下行链路进行同步设置，使上层设备的故障迅速传达给下层，从而触发链路切换，避免因上行链路故障无法被下层设备感知而出现的流量丢失。

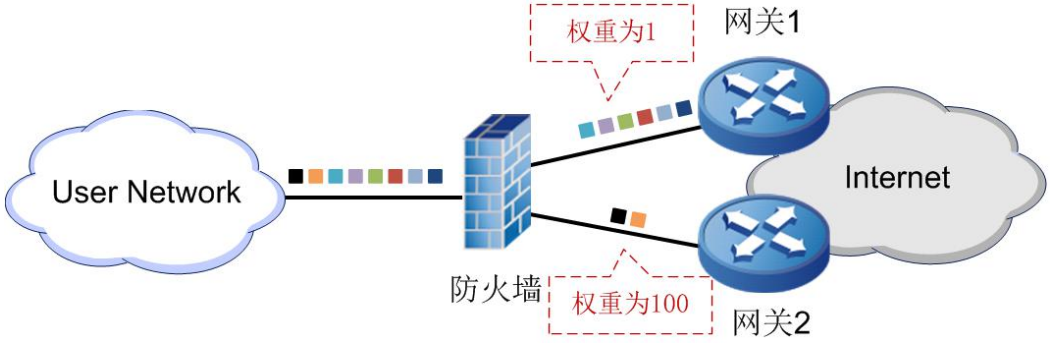
图 2-16 接口联动示意图



静态路由负载均衡

防火墙支持基于多条静态路由的流量均衡负载。用户可以根据实际组网，配置多个网关。多个网关之间使用路由权重来衡量优先级，当用户配置多条静态路由时，权重越高，分配的会话数越多。

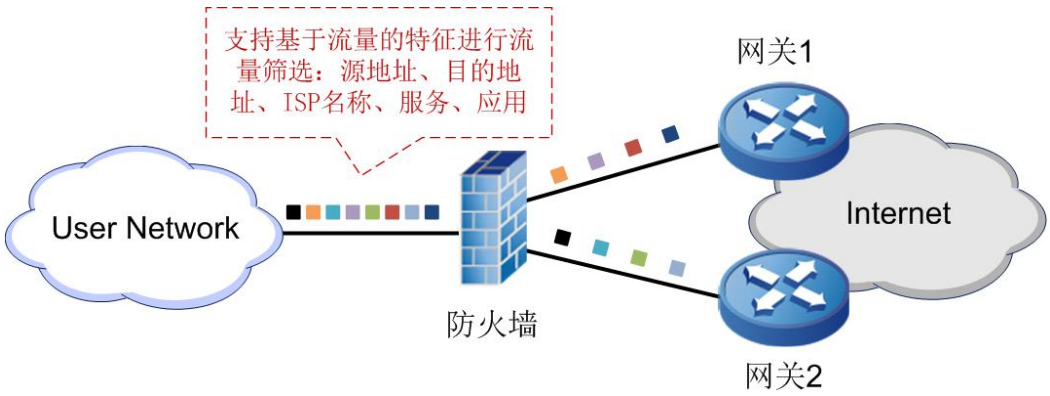
图 2-17 静态路由负载均衡示意图



策略路由负载均衡

当用户拥有 2 条及以上的出口网络，就可以通过策略路由对流量进行筛选，实现基于不同流量的特征，从不同出口去访问互联网的目的，同时可以实现链路负载分担。

图 2-18 策略路由负载均衡示意图



防火墙不但可以根据流量特征进行分流，对于相同特征的流量，还可以配置多个网关，并基于不同的策略进行流量均衡负载。

防火墙支持的策略路由流量均衡负载方式如表 2-2 所示。

表 2-2 策略路由流量均衡负载方式

均衡负载方式	说明
源地址目的地址哈希	对源地址和目的地址进行哈希，同一个源地址同一个目的地址的数据包总是从相同的网关出去。
轮询	将需要转发的数据包按照权重值所配置的比例，轮流分配给每一个网关。
源地址哈希	对源地址进行哈希，同一个源地址的数据包总是从相同的网关出去。避免一个客户端的不同的请求被分配到不同的网关进行转发。
目的地址哈希	对目的地址进行校验，去往同一个目的地址的数据包总是从相同的网关出去。避免去往同一个目的地址的请求被分配到不同的网关进行转发。
源地址轮询	对源地址进行哈希，同一个源地址的数据包总是从相同的网关出去。同时，不同的源地址按照权重值配置的比例轮流分配给每一个网关。
备份	当具有多个网关时，依优先级由高到低来选择网关，优先级高的链路不通时，再选择优先级低的链路，依此类推。当优级较高的网关恢复通信时，再切回优先级较高网关。 同一优先级下，有多个网关时，主链路由多个出接口轮询组成。当主链路中所有出接口都不通后，再切换至备份链路。

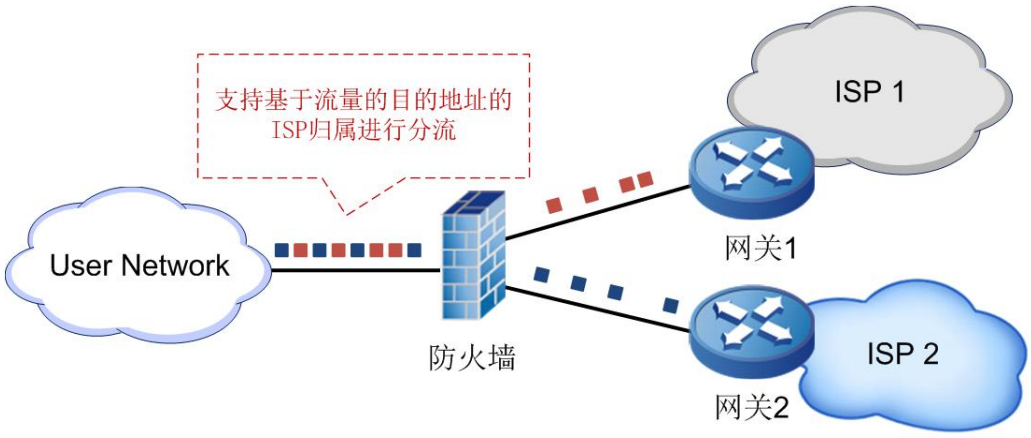
均衡负载方式	说明
最优链路带宽负载	指定网关地址的同时，还需要指定网关对应的带宽大小，网关的带宽大小主要依据为出口带宽的大小。带宽最大的出口将被防火墙选定为最优链路。
最优链路带宽备份	指定网关地址的同时，还需要指定网关对应的带宽大小，网关的带宽大小主要依据为出口带宽的大小。 最优链路带宽备份在新建会话进入防火墙时，会根据比较当前各个网关的剩余带宽，选择剩余带宽最大的那条链路进行转发。
随机	具备多个网关时，随机选择其中一个网关进行转发。映射为权重值相等的轮询算法。
流量均衡	如果采用简单的轮循或随机均衡算法，每一出接口上承担的流量大小可能会产生极大的不同，这样的结果并不会达到真正的负载均衡。 流量均衡算法对有负载的每一出接口都有一个数据记录，记录的内容是当前出接口的负载流量大小，当有新的数据包转发时，将把数据包分配给流量负载最少的节点，使均衡更加符合实际情况,负载更加均衡。
时延负载	时延负载会根据探测结果反馈的延迟时间，选取多个网关中延迟最小的出口进行转发。
跳数负载	跳数负载会根据探测结果反馈的跳数值，选取多个网关跳数最小的出口进行转发。

ISP 路由负载均衡

防火墙支持 ISP 信息库，信息库中保存了中国电信、中国联通、中国移动、教育网等运营商目的 IP 地址。通过在 ISP 路由中直接指定运营商名称，可以实现通过不同运营商的出口链路访问相应运营商的 IP 地址。

同时，对于相同的 ISP 运营商，也支持配置多个网关。多个网关之间使用路由权重来衡量优先级，当用户配置多条静态路由时，权重约高，分配的会话数越多。

图 2-19 ISP 路由负载均衡示意图



2.7 全面、智能的路由功能

2.7.1 全面的路由功能

防火墙支持全面、完善的路由功能。扩大了防火墙系统工作在路由模式下时的网络适应能力及对 IPv6 网络的适应能力。

- 支持静态路由功能，包括 IPv4 静态路由和 IPv6 静态路由；
- 支持静态多播路由及动态多播路由；
- 支持多种动态路由，如 RIP、OSPF、BGP、RIPng、OSPFv3、BGP4+。

2.7.2 精确的多出口 ISP 路由智能选路

ISP 路由功能主要为用户提供基于不同运营商的路由出口选择策略。常用于用户使用多出口上网，并且多个出口对应着多个运营商的场景。

往往跨运营商访问服务的速度会稍慢一些，因此我们希望如果目的地址是去往电信的，那我们就将该目的地址添加一条对应的静态路由指向电信出口。但是运营商的地址范围通常过大，如果手工添加静态路由，对用户来说会是一件非常麻烦且耗时的工作。

ISP 路由智能选路功能提供了快速添加运营商路由的方法，同时支持在策略路由中引用 ISP 路由。用户可以直接选用防火墙预设置的运营商地址信息，或者将运营商的地址范围写成文本文档，导入到防火墙系统中，为每一个运营商添加一条对应出口的 ISP 路由即可。

2.7.3 对称路由保证来回路径一致

防火墙支持对称路由功能。用户可以通过启用接口的对称路由功能，实现用户从哪里进来访问的数据，从哪里再返回出去。例如：用户内网对外提供一个 http 服务，同时用户申请了联通和电信两个出口。当联通的用户从联通出口进来访问 http 服务时，对称路由功能可以让服务器返回给用户的应答数据也从联通出口出去。当电信的用户从电信出口进来访问 http 服务时，对称路由功能可以让服务器返回给用户的应答数据也从电信出口出去。保证数据来回路径的一致性。

2.7.4 高适应性的路由负载均衡算法

防火墙支持在多出口的环境中根据用户实际需求，匹配多种方式的负载均衡算法，包括备份、轮询、源地址哈希、源地址目的地址哈希、目的地址哈希、源地址轮询、最优链路带宽负载、最优链路带宽备份、随机、流量均衡、时延负载、跳数负载等十二种。可以实现基于权重的路由负载、基于延迟的路由负载、基于会话的路由负载、基于流量的路由负载，满足用户各种场景。

2.8 全面的 SSL 解密防护

2.8.1 SSL 解密

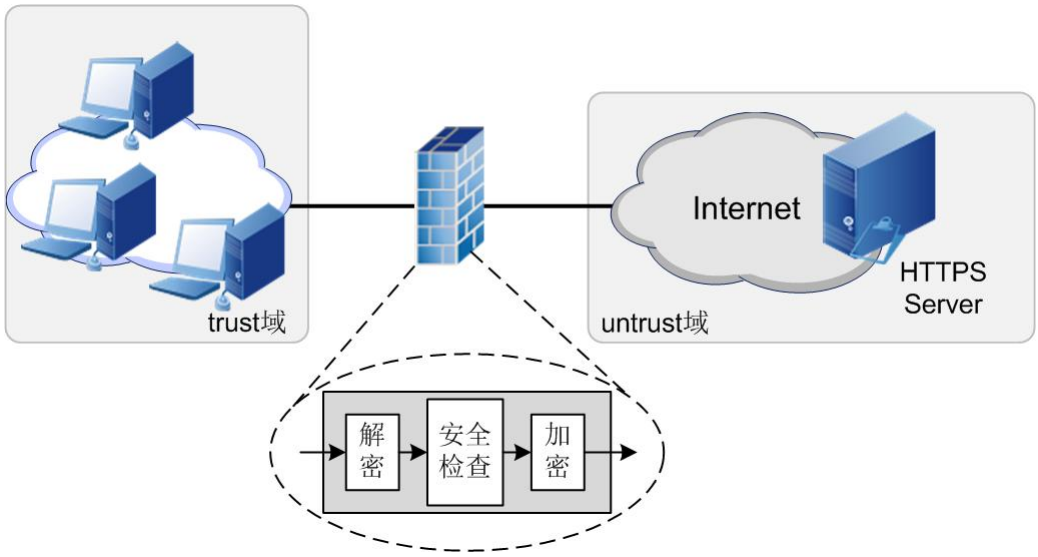
SSL 协议是在互联网上广泛应用于交易安全性保障的一种重要技术。在一般情况下，HTTP 采用明文的方式在互联网上进行传输，存在被非法窃听的风险。为了消除这一隐患，可采用 SSL 协议对 HTTP 协议进行加密（即 HTTPS），以确保在整个数据传输过程中的信息安全性。

但是，加密流量也对防火墙设备的安全检测功能带来的巨大挑战，因为数据内容处于完全加密的状态，处于连接中间位置的防火墙设备无法对应用数据进行分析，检测应用数据可能存在威胁、病毒或未授权的数据传输等。

SSL 解密功能的出现为 SSL 加密流量威胁防御带来了转机。如图 2-20 所示，防火墙使用 SSL 解密功能可以对 SSL 加密流量进行解密，再对解密后的流量做内容安全检查和过滤。

- 对于通过内容安全检查的流量，即没有命中关键字，防火墙会重新加密，确保经过防火墙解密后的流量在离开防火墙时依旧安全。
- 对于没有通过内容安全检查的流量，即命中关键字，防火墙会实施阻断操作，有效拦截基于 SSL 的加密流量攻击和信息泄露。

图 2-20 SSL 解密功能



2.8.2 SSL 入站检查

防火墙支持旁路模式下的 SSL 入站检查功能，可以对防火墙后的服务器进行保护，当有客户端使用 HTTPS 等协议访问服务器时，防火墙可以对访问数据进行威胁检测。

2.9 丰富的 VPN 隧道类型

防火墙支持多种形式的 VPN 隧道，完全覆盖 Client-to-Site 和 Site-to-Site 应用场景。包括：PPTP VPN、L2TP VPN、GRE、IPSec VPN 和 SSL VPN，并支持 L2TP over IPSec VPN 和 GRE over IPSec VPN。

同时，防火墙支持多种类型的 6in4 隧道，包括手工隧道、isatap、6to4 隧道、DS-Lite，保证 IPv6 网络到 IPv4 网络的访问。

2.10 强大的识别功能，实现精细化管控

2.10.1 用户识别

用户是网络使用的主体，也是进行管控的基础。基于用户的上网行为管控的核心是对网络用户的识别和分类。

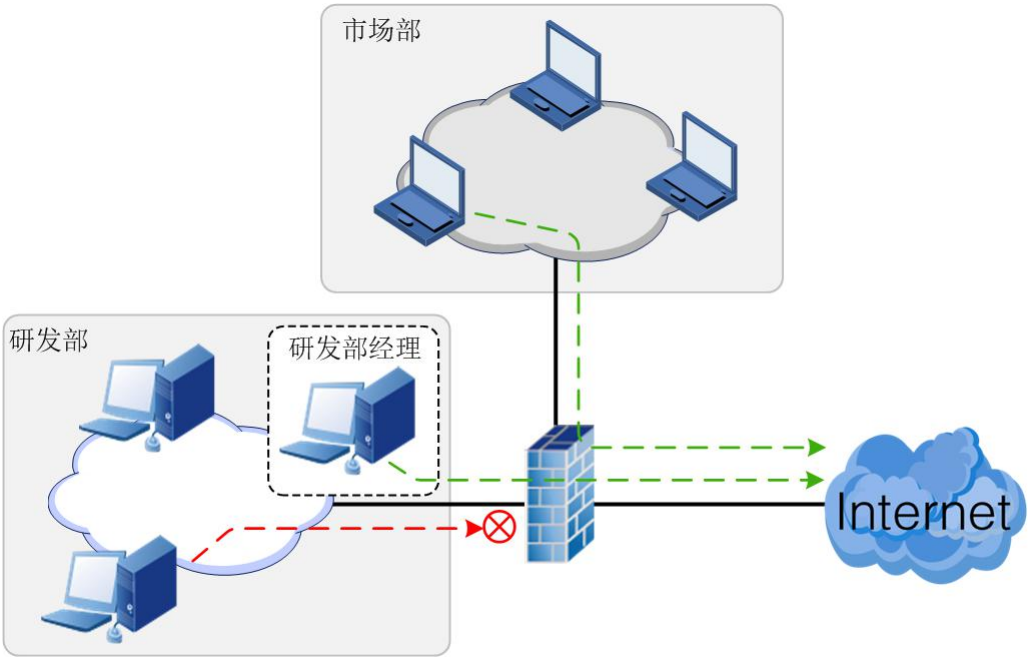
防火墙支持基于用户的行为管控策略，方便了管理员对企业内部网络行为进行审计，管理员面对的不再是单调的 IP 地址，而是非常具体的人名，能够很直观的发现网络中的违规者。从而提高网络管理效率，保证信息安全。

基于用户的识别和管控与 BYOD 有着天然的适应性，因为无论用户使用什么终端访问网络，也无论用户上网使用的 IP 是多少，均可以直接映射成为用户名的形式，方便网络管理员进行审计。

如图 2-21 所示，网络管理员可以基于不同颗粒度进行上网行为管控。

- 基于“单个用户”进行管控。管理员可以定义单个用户拥有访问 Internet 的权限及时间，方便在相同用户组内部，更精细化地进行权限控制，例如：在研发部门内部，经理有访问 Internet 的权限，其他员工则没有。
- 基于“用户组”进行管控。管理员可以将现实中的部门映射为系统中的用户组，并定义用户组拥有访问 Internet 的权限。该方案可以实现用户行为的批量配置。当有员工加入或退出部门时，只需在用户组内增加或删减即可，简化配置。
- 基于“用户角色”进行管控。管理员可以将不同的用户根据角色进行划分，并定义用户角色拥有访问 Internet 的权限。该方案可以实现用户行为的批量配置。当有员工加入该角色时，只需在角色中增加或删减即可，简化配置。

图 2-21 基于用户的识别和管控



2.10.2 服务识别

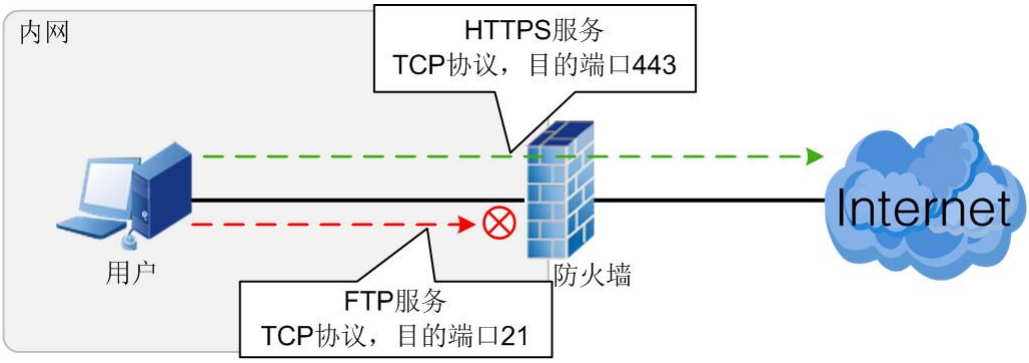
防火墙支持基于 TCP 和 UDP 协议，通过源端口号、目的端口号以及协议号进行服务识别。

防火墙内置有常用协议的服务库，用户在使用时可以直接选择库中的协议。还支持自定义服务，通过 TCP、UDP 协议的源端口号和目的端口号来定义服务。

缺省的服务和自定义的服务可以作为安全策略的一个属性，实现基于服务的精细化流量管控。

如图 2-22 所示。某内部网络禁止用户访问 FTP 服务。只要在防火墙上基于 FTP 服务（即 TCP 协议，目的端口为 21 的服务）进行管控，配置相关的安全策略，即可实现。

图 2-22 基于服务的识别和管控



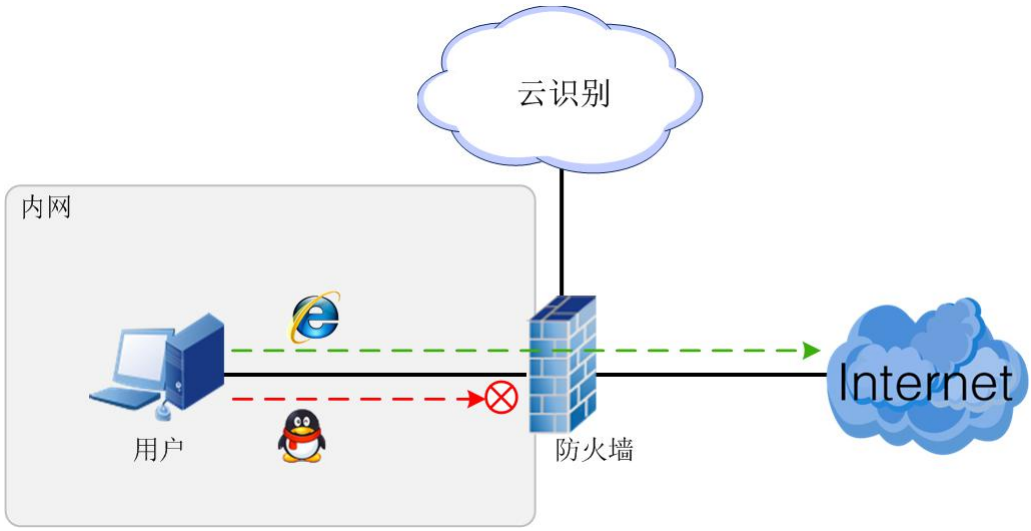
2.10.3 应用识别

防火墙支持应用识别库，包括 7000+应用特征。通过应用识别库，防火墙可以对流量进行应用识别。

基于应用的流量识别和管控，用于限制网络内部的用户使用某种指定的应用程序，该方法在不限制用户访问 Internet 的前提下，能够差别化地限制某些影响工作效率或占用大量带宽应用的使用。例如：QQ、P2P 软件等。

如图 2-23 所示。某内部网络禁止用户使用 QQ 软件。只要在防火墙上基于 QQ 应用进行行为管控，配置相关的安全策略，即可实现。

图 2-23 基于应用的识别和管控



2.10.4 内容识别

防火墙支持基于深度内容识别的行为管控策略，用于限制企业内部网络机密信息的传播，从而降低公司机密泄露的风险，保证信息安全。

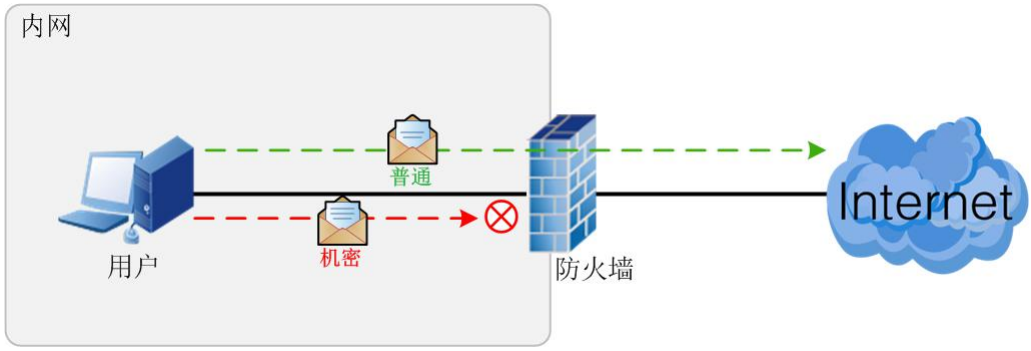
内容识别功能即支持文件内容识别，也支持应用内容识别。

- 文件内容识别：指对文件的文件名和内容进行识别，例如对用户上传 Word 文档时，系统对文档名称和文档的内容进行识别。
- 应用内容识别：指对应用的内容进行识别，例如用户在网上发帖/发微博时，系统对用户发帖的标题和内容进行识别。

如图 2-24 所示，当用户向外网传播公司机密信息时，防火墙接收到相关报文后，对报文的内容进行扫描和识别，如果报文中带有机密信息字段或不符合法律规定的内容字段，会阻断该报文。

同时，正常的、无相应字段的报文不受影响，能够被正常发送和接收。

图 2-24 基于内容的识别和管控



2.10.5 URL 识别

防火墙支持基于 URL 的识别和管控，用于限制企业内部网络用户访问某些特殊的 URL，可以起到提升工作效率、降低法律风险的作用。例如禁止访问色情类、反动类的 URL 等。

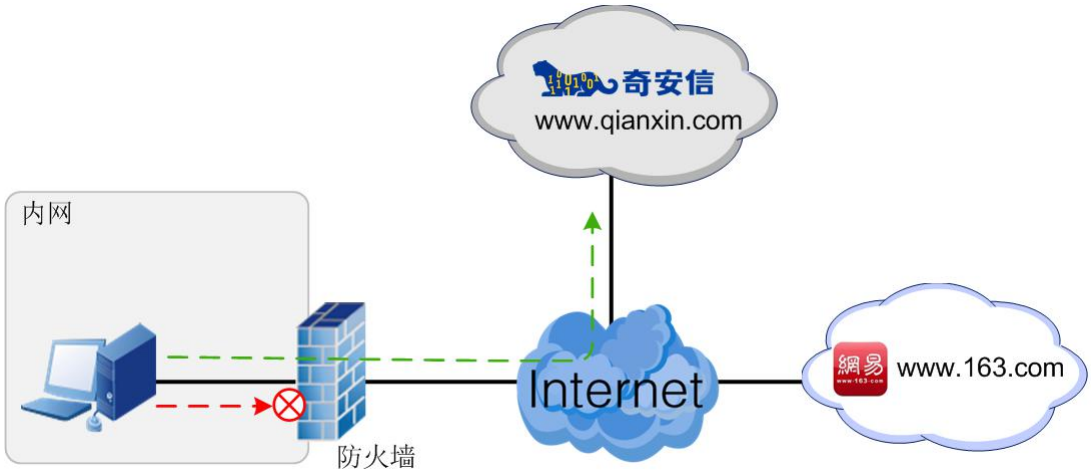
防火墙支持自定义 URL，系统通过检测 HTTP 请求头中的 URL 字段，对照配置的管控策略来允许或拒绝请求。

- 对允许的请求，用户直接访问该站点。
- 被禁止的请求，向用户发送一个禁止访问的信息。

此外，还可通过系统自带的 URL 分类库来拒绝用户对某一类站点的访问。

如图 2-25 所示。某内部网络禁止用户访问 www.163.com。只要在防火墙上基于 URL 进行行为管控，配置相关的安全策略，即可实现。

图 2-25 基于 URL 识别和管控



2.10.6 行为识别

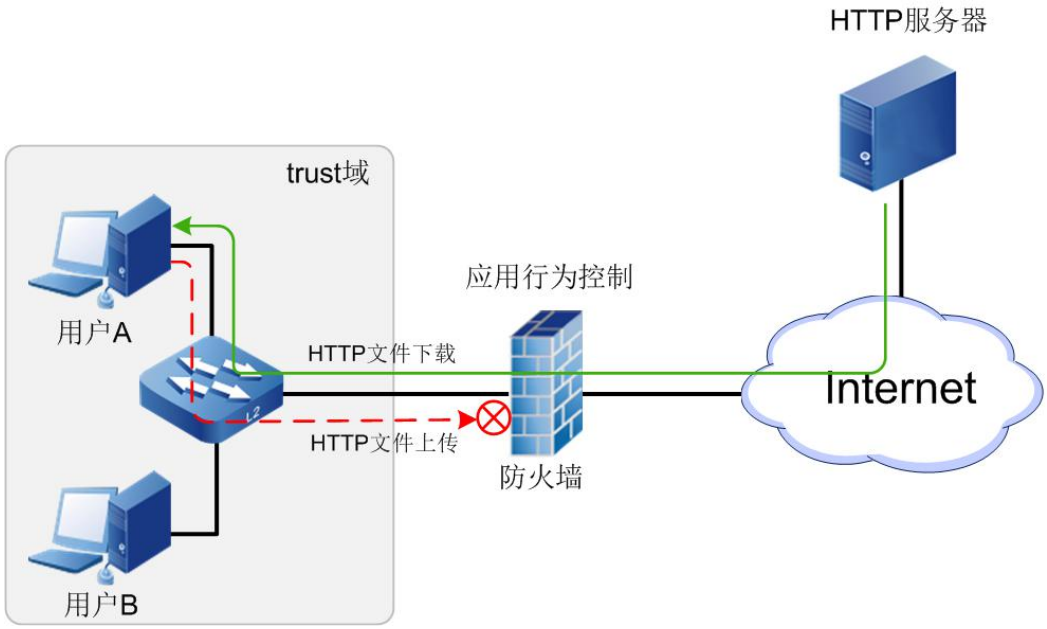
防火墙的应用行为控制功能支持对用户的 HTTP 行为、FTP 行为、SMTP 行为、POP3 行为、IMAP 行为和 Telnet 行为进行精确的控制。

在企业内部通常需要对内网用户的行为进行管理，不同的用户使用协议访问网络资源需要不同的权限，同一用户在不同的时间段具有的权限往往也不同。防火墙的应用行为控制能够很好的满足上述需求。

如图 2-26 所示，防火墙作为企业的出口网关部署在出口处，通过在防火墙上配置应用行为控制功能，当内网用户访问外网时，能够有效管理内网用户的行为。

在防火墙上创建多个应用行为控制配置文件，每个应用行为控制配置文件用来控制用户具有不同的权限。然后通过在安全策略里面引用应用行为控制配置文件、用户和时间段（工作时间、非工作时间）等对象，可以达到对内网用户的行为差异化、精细化管理的目的。

图 2-26 应用行为的识别和管控



2.10.7 地理位置识别

防火墙支持地理位置识别功能，支持识别国内和国际 IP 地址，并将 IP 地址映射称为具体的地址位置。

用户可以将地理位置作为配置安全策略的一个属性。通过地址位置识别用户可以了解到不同地区当前的网络使用情况，查看基于地理位置的流量趋势、威胁趋势等，从而针对不同的地理位置来调整防火墙策略，为用户的安全策略管理提供一个新的控制角度。

2.10.8 精细化的安全策略

防火墙的安全策略是防火墙的核心功能，是防火墙实现访问控制的基础。

防火墙支持基于状态检测和应用层数据识别的动态包过滤技术。通过源安全域、目的安全域、源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、地理位置、用户、服务、应用、时间等维度对数据进行识别，将用户需要进行过滤及控制的数据流分离，并实现精细管控。

同时，防火墙支持对相应的数据实现反病毒、漏洞防护、防间谍软件、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控的一体化策略配置。

2.11 深度安全检测及 DLP，保护网络安全

2.11.1 概述

防火墙具有数据深度安全检测能力和攻击防御能力。主要包括：

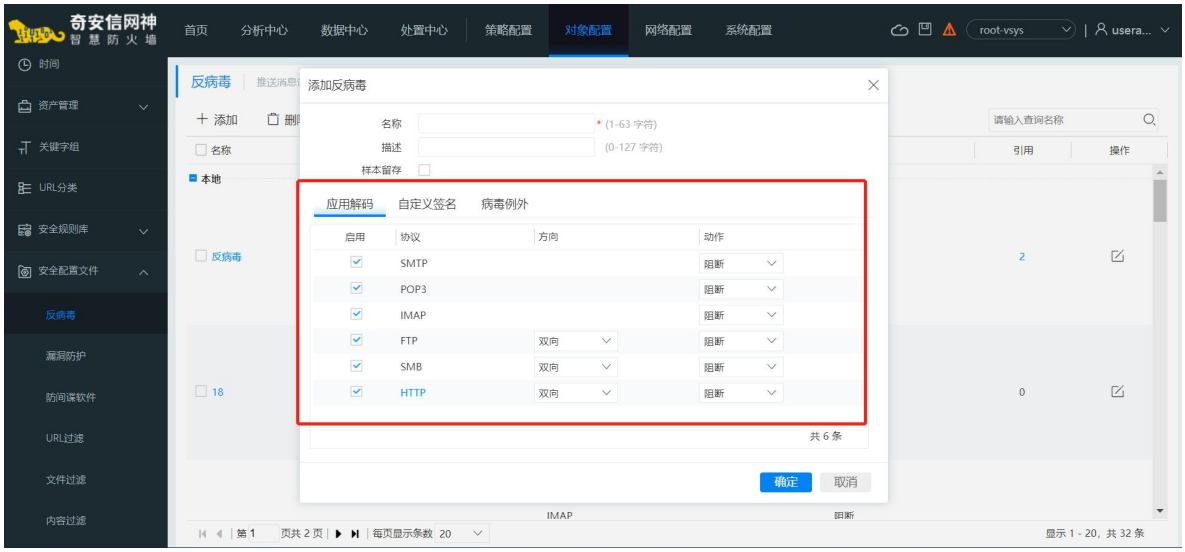
- 攻击防护：支持 DoS/DDos 防护、畸形报文防护、DHCP 防护等。
- 入侵防护：支持漏洞防护、间谍软件防护、Web 防护、病毒防护等。
- DLP 方面：支持邮件过滤、文件过滤、内容过滤等。
- 未知威胁防护：支持威胁情报、0-day 威胁防护、APT 未知威胁防护等。

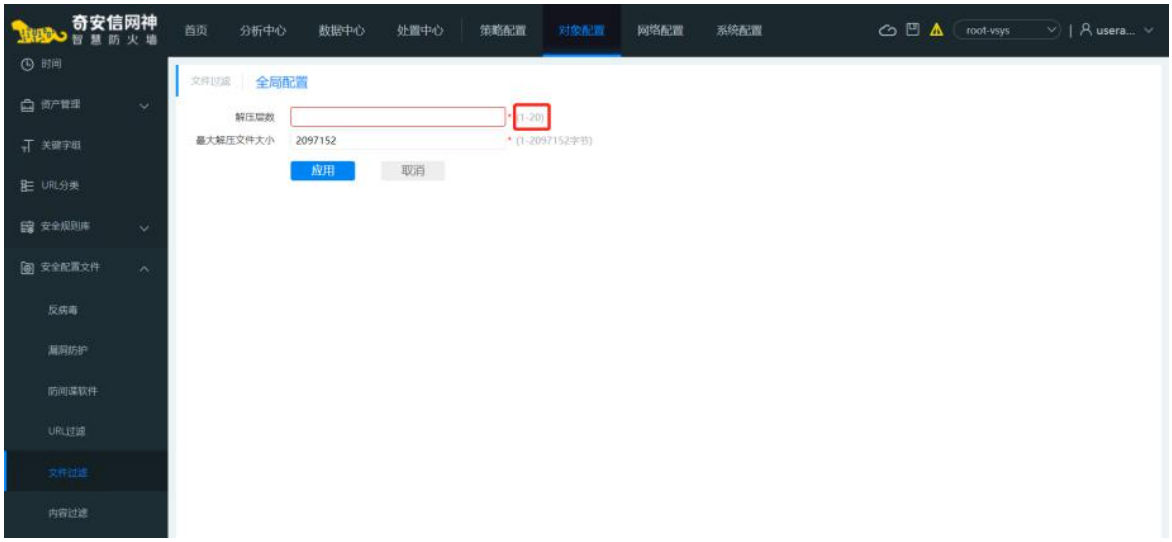


2.11.2 全面的应用层攻击防护能力

防火墙基于安全域，支持多种类型的攻击防护。

- Flood 防护。包括 SYN Flood、ICMP Flood、UDP Flood、IP Flood、DNS Flood 和 HTTP Flood 防护。
- 恶意扫描防护。包括 Tracert 扫描、IP 地址扫描和端口扫描。
- 欺骗防护。包括 IP 欺骗和 DHCP 防护。
- 异常包防护。包括 ping of death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常和 IP 分片等。
- ICMP 管控。包括禁止 ICMP 分片、禁止路由重定向报文、禁止不可达报文、禁止超时报文和 ICMP 报文大小限制。
- ICMPv6 管控。包括禁止不可达报文、禁止数据包太大报文、禁止超时报文、禁止参数问题报文、禁止分片和 ICMPv6 报文大小限制。
- ICMPv6 扩展头防护。包括扩展头顺序检查、扩展头次数检查、扩展头个数检查和禁止扩展头类型（逐跳选项头、目的地址选项头、路由选项头、分片选项头、ESP 选项头、AH 选项头和 None 选项头）。
- IPv4 SYN Cookie 和 IPv6 SYN Cookie。
- 病毒防护。包括流模式文件扫描技术，对 HTTP、SMTP、POP3、IMAP、FTP 等多种协议类型的病毒进行查杀，包括木马、蠕虫、脚本病毒等进行有效控制和查杀，可对 20 级的压缩文件进行解压查杀。





由于常见的攻击方式掺杂了大量的组合式洪攻击，攻击者实际上是在消耗被攻击者的性能资源，因此防火墙系统强大的性能支撑，也保证了在大量攻击消耗防火墙性能的时候不会成为用户网络中的瓶颈，给予了防火墙攻击防护模块和其他模块坚实的性能基础。

2.11.3 先进的多维动态特征异常检测引擎

防火墙采用全新先进的多维动态特征异常检测引擎，抛弃原有的异常行为特征码静态表达的方式，将异常行为、恶意行为特征码通过多维度提炼，动态进行表达，使得特征表达更加全面、精准、有效，极大提高了防火墙入侵防御系统的命中质量，解决了传统设备检测命中率高，但是误报率同样高的问题。

防火墙漏洞特征库中支持按漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。

防火墙支持状态检测技术，对安全域、IP 地址、端口、协议、用户、应用、时间等维度对数据报文进行深度检测，阻断违规数据访问。

防火墙支持基于 IMAP、FTP、RDP、VNC、SSH、Telnet、Oracle、MySQL、SQL Server 等应用协议进行深度检测与防护。

防火墙支持 CC 攻击检测和防护功能。

防火墙支持对文件传输行为进行安全过滤，基于上传、下载、双向的文件内容过滤，内容过滤类型，支持网页、脚本、压缩文件、图片、可执行文件、适配、文本等常见文件类型。

防火墙具备安全策略有效性分析功能，分析内容包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。支持策略生命周期管理功能，对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。

防火墙支持对常见 Web 应用攻击防御，攻击类型支持跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、webshell、网站扫描、网页木马等类型攻击行为。

2.11.4 灵活的自定义漏洞/间谍软件特征功能

防火墙支持自定义基于 TCP、UDP 和 HTTP 协议的漏洞及间谍软件特征，并根据各协议的报文结构，指定一个或多个字段的特征值，这些特征值可以被以文本的形式或正则表达式的形式进行匹配，同时支持是否按顺序对这些特征值进行匹配检测。支持自定义漏洞及间谍软件的源端口范围及目的端口范围。

2.11.5 多维度的 DLP 数据防泄漏

防火墙提供内容过滤、文件过滤、URL 过滤、网络行为管理功能，从而实现对用户的网络行为进行管控。行为管控策略不仅支持精确到 IP 地址，更可精确到用户。同时，在内容过滤中还实现了对敏感信息泄露的防护。

内容过滤支持基于常见的协议与应用的内容过滤。

- 支持基于关键字的内容过滤。关键字支持文本匹配或正则表达式匹配。
- 协议包括：FTP、HTTP、SMTP、POP3、IMAP、SMB。
- 文件类型包括：html、txt、doc、docx、xls、xlsx、ppt、pptx、pdf、rtf、xml、tex、chm、sxc 和 ps。

文件过滤支持基于常见的协议与应用的文件过滤。

- 协议包括：FTP、HTTP、SMTP、POP3、IMAP、SMB。
- 支持 30+种文件类型，包括：html、doc、docx、xls、xlsx、ppt、pptx、pdf、troff、rtf、xml、tex、mime、pst、hlp、chm、h1s、umd、wdl、cebx、sxc、fdf、tnef、mbx、zip、gz、rar、7z、bz2、cab、ps、tar、cpio、deb。
- 支持对压缩文件进行扫描和过滤，最大解压层数为 6 层。

行为管控支持对 HTTP、SMTP、POP3、IMAP、FTP、TELNET 协议的关键命令、关键字内容进行管理，支持 SMTP、POP3、IMAP 邮件协议发件人、收件人的地址黑白名单设置。

2.11.6 强大的威胁情报渗透

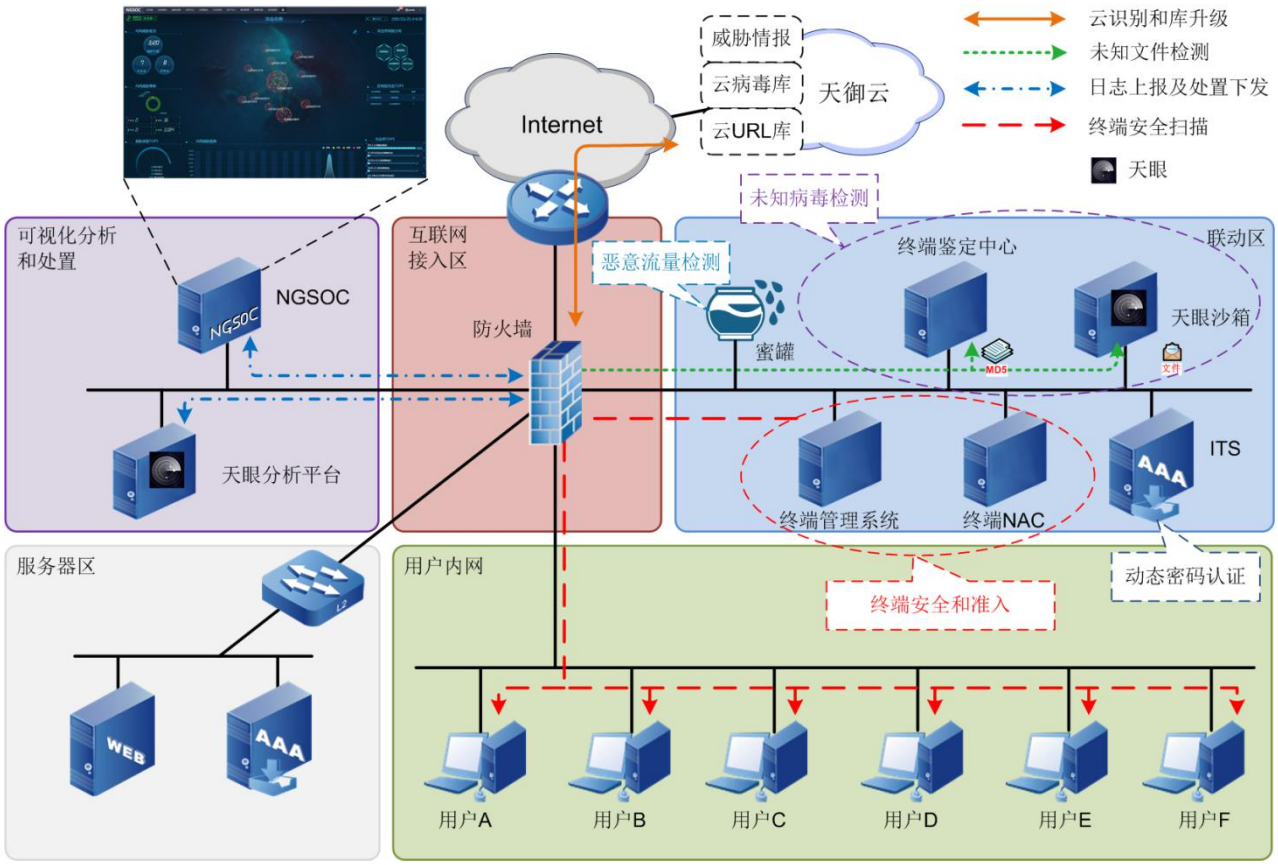
防火墙支持强大的本地威胁情报检测功能，方便对用户网络中的未知威胁进行检测和识别。

威胁情报要基于海量数据才能生产出来，奇安信基于人工智能自学习的自动化数据处理技术，依靠以顶尖研究资源为基础的多个国内高水平安全研究实验室，为未知威胁的最终确认提供专业高水平的技术支撑。

- 所有大数据分析出的未知威胁都会通过专业的人员进行人工干预，做到精细分析，确认攻击手段、攻击对象以及攻击的目的。
- 通过人工智能结合大数据知识以及攻击者的多维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征‘跟踪’攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供终端平台使用的威胁情报。

2.12 多系统联动防护，构建立体式防护体系

防火墙支持与终端管理系统、天眼、NGSOC、ITS、蜜罐、天御云等系统进行联动，实现基于“云-界-端”的立体化、全网网络行为的检测和安全防护、定位并拦截已知威胁和未知威胁。



2.12.1 防火墙和终端系统联动

防火墙支持与终端管理系统、终端鉴定中心和终端 NAC 进行联动，实现终端管控、私有云病毒查杀和终端准入功能。

- 终端管控。防火墙通过与终端管理系统联动，结合终端管理系统对用户 PC 终端的安全扫描结果，根据用户终端的高、中、低风险等级，实现终端管控。同时，还支持对未安装奇安信安全助手的终端进行管控，以保证杀毒软件的安装覆盖率。
- 私有云病毒查杀。防火墙通过与终端鉴定中心联动，将未知文件的 MD5 码发送给终端鉴定中心进行识别，利用云端病毒库，提高病毒检出率。
- 终端准入。防火墙和终端 NAC 进行联动，可以利用防火墙的精细化管控能力，细粒度地对用户的网络访问行为进行管控。以实现核心业务访问准入、入网安全合规性要求、网络实名制认证管理、网络边界接入安全防护等功能。

2.12.2 防火墙和天眼系统联动

防火墙支持与天眼分析平台、天眼沙箱进行联动，整合天眼深度检测能力与防火墙实时阻断能力，实现威胁检测、一键处置、沙箱联动等功能。

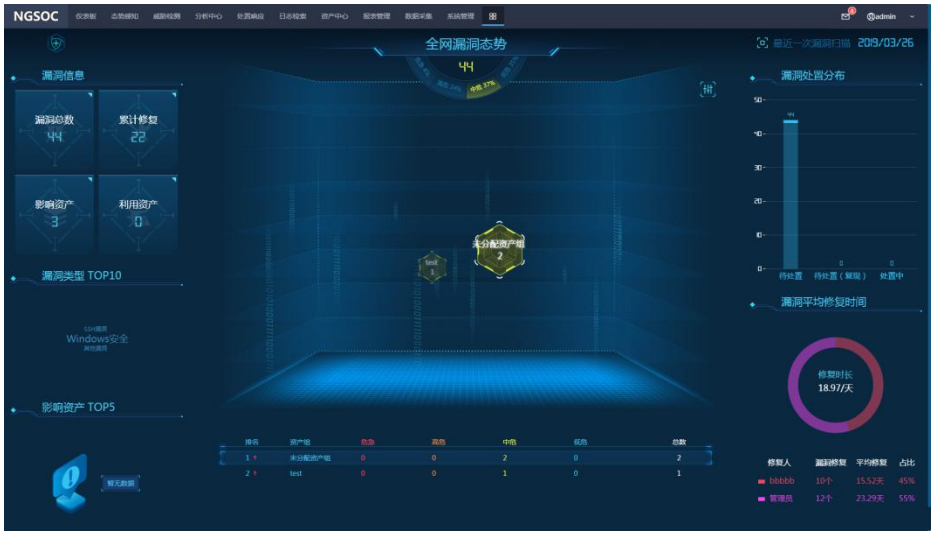
- 深度检测。防火墙通过和天眼分析平台联动，将通过防火墙的流量，以日志形式上传到天眼分析平台做深度检测和分析，充分利用天眼的深度检测能力。
- 一键处置。天眼接收防火墙的日志后进行深度分析，发现威胁后自动或手动下发处置策略。防火墙支持响应天眼分析平台的处置策略，完成对发现威胁的处置和拦截，从而对用户访问外网的流量提供安全保障。
- 沙箱联动。防火墙支持与天眼沙箱进行联动，将未知威胁文件发送到沙箱检测，并支持响应沙箱的检测结果，对沙箱检测发现的未知病毒进行处置和拦截。作为本地病毒库、云端病毒库的补充，沙箱能够极大地提升防火墙的病毒防护能力，尤其是对未知病毒的防护能力。

2.12.3 防火墙和 NGSOC 系统联动

防火墙支持与 NGSOC 系统进行联动，整合 NGSOC 系统数据深度挖掘和态势感知能力，实现用户网络状态和威胁的可视化。同时支持响应 NGSOC 平台下发的处置策略，完成威胁的一键处置。

- 态势感知。防火墙支持将采集到的网络流量，以日志形式上传到 NGSOC 平台做深度分析。结合 NGSOC 深度数据挖掘并实现可视化态势感知。

- 防火墙支持响应 NGSOC 平台的处置策略，完成对发现威胁的处置和拦截，从而对用户访问网络的流量提供安全保障。



2.12.4 防火墙和天御云系统联动

天御云作为云端大数据库，所拥有的库容量和实时状态，是防火墙单机无法比拟的。

防火墙支持与天御云进行联动，使用云端的 URL 库、病毒库、应用识别库等资源作为防火墙本地库的补充和扩展，提升对应用、威胁的识别深度和广度。

同时，对于未知病毒，还支持上传至云端沙箱进行识别。

2.12.5 防火墙和 ITS 系统联动

ITS（身份令牌服务平台）是奇安信集团为了解决新型 IT 环境下身份安全问题而推出的一款产品。该产品采用了指纹技术、环境安全技术、身份识别技术、国密算法等多项核心技术，实现了动态密码、多因子认证等功能。

防火墙支持和 ITS 系统联动，实现基于“动态密码”的用户身份认证策略。基于 ITS 的“动态密码”认证策略，能够对用户身份进行更严格的验证，极大地提高用户的安全，主要应用场景有：

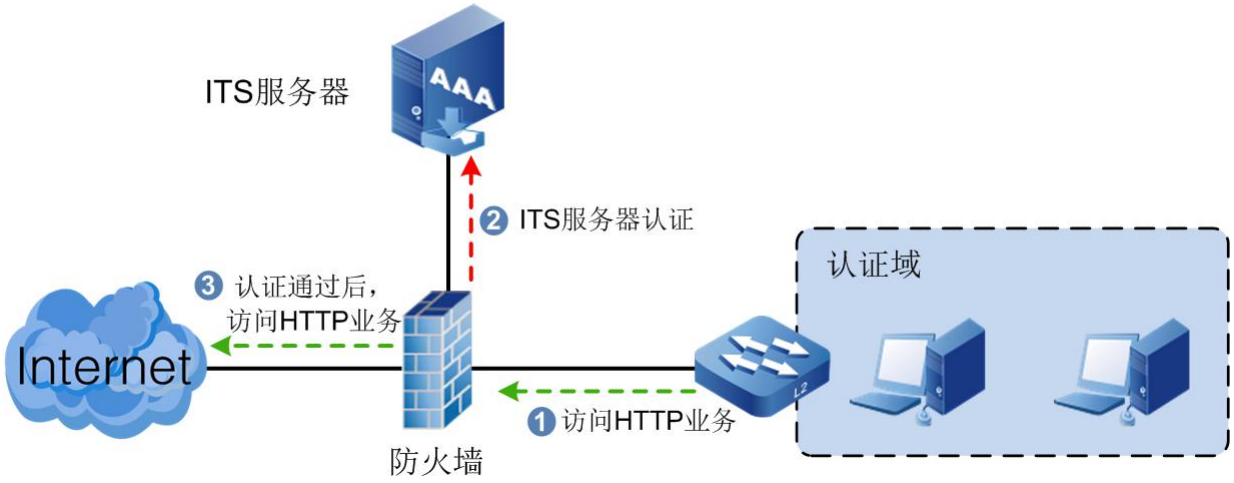
- Web 用户认证应用场景
- SSL VPN 用户认证应用场景
- 防火墙管理员认证应用场景

Web 用户认证应用场景

防火墙和 ITS 联动认证解决方案适用于用户 Web 上网认证场景中。在该场景下，用户可以通过天鉴 ID 软件获取实时的动态密码，并通过动态密码完成认证和上网，极大地提高了用户的安全性。

如图 2-27 所示，防火墙内网用户在访问 Internet 之前，必须基于动态密码通过 ITS 服务器的认证。认证成功后，防火墙会记录访问者使用的用户和 IP 地址之间的对应关系，并放行用户流量，完成用户认证。

图 2-27 Web 认证应用场景

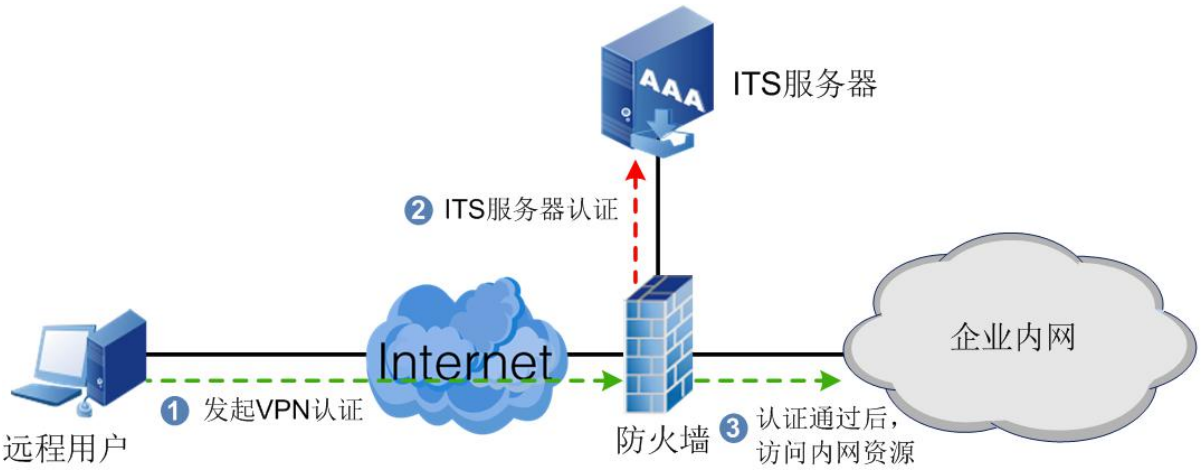


SSL VPN 用户认证应用场景

防火墙和 ITS 联动认证解决方案适用于 SSL VPN 用户认证场景中。在该场景下，用户可以通过天鉴 ID 软件获取实时的动态密码，并通过动态密码完成 SSL VPN 身份认证，极大地提高了 SSL VPN 的安全性。

如图 2-28 所示，外网用户在进行 SSL VPN 拨号时，支持基于动态密码通过 ITS 服务器的认证。认证成功后，防火墙会记录访问者使用的用户和 IP 地址之间的对应关系，完成用户认证，并允许用户访问内网。

图 2-28 SSL VPN 认证应用场景

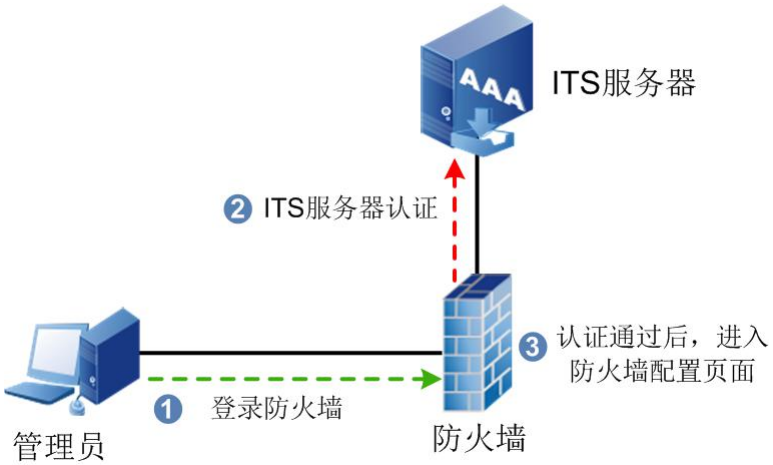


防火墙管理员认证应用场景

防火墙和 ITS 联动认证解决方案适用于防火墙管理员认证场景中为管理员提供双因素认证功能。在该场景下，用户可以通过天鉴 ID 软件获取实时的动态密码或短信动态密码认证，并通过本地账号密码和动态密码完成管理员用户认证方式登录产品的管理界面，极大地提升防火墙本身的安全性。

如图 2-29 所示，当管理员登录防火墙管理界面时，必须基于动态密码通过 ITS 服务器的认证。认证成功后，防火墙会允许管理员登录，并完成管理员登录 IP 等信息的记录。

图 2-29 防火墙管理员认证应用场景



2.12.6 防火墙和蜜罐联动

防火墙支持网络诱捕技术，可以感知网络中的扫描行为，并将可疑流量诱骗至蜜罐进行深度互动检测和分析，并基于分析结果，对发现的攻击流量进行阻断，从而保护现有业务网络。

蜜罐联动功能支持多种诱捕方式。包括：基于五元组静态诱捕、基于不存在 IP 地址的动态诱捕、基于不存在端口的动态诱捕和基于 IOC 的恶意域名诱捕。

根据防火墙的部署位置，可以对公网流量或内网流量进行诱捕。

图 2-30 诱捕实现流程-公网

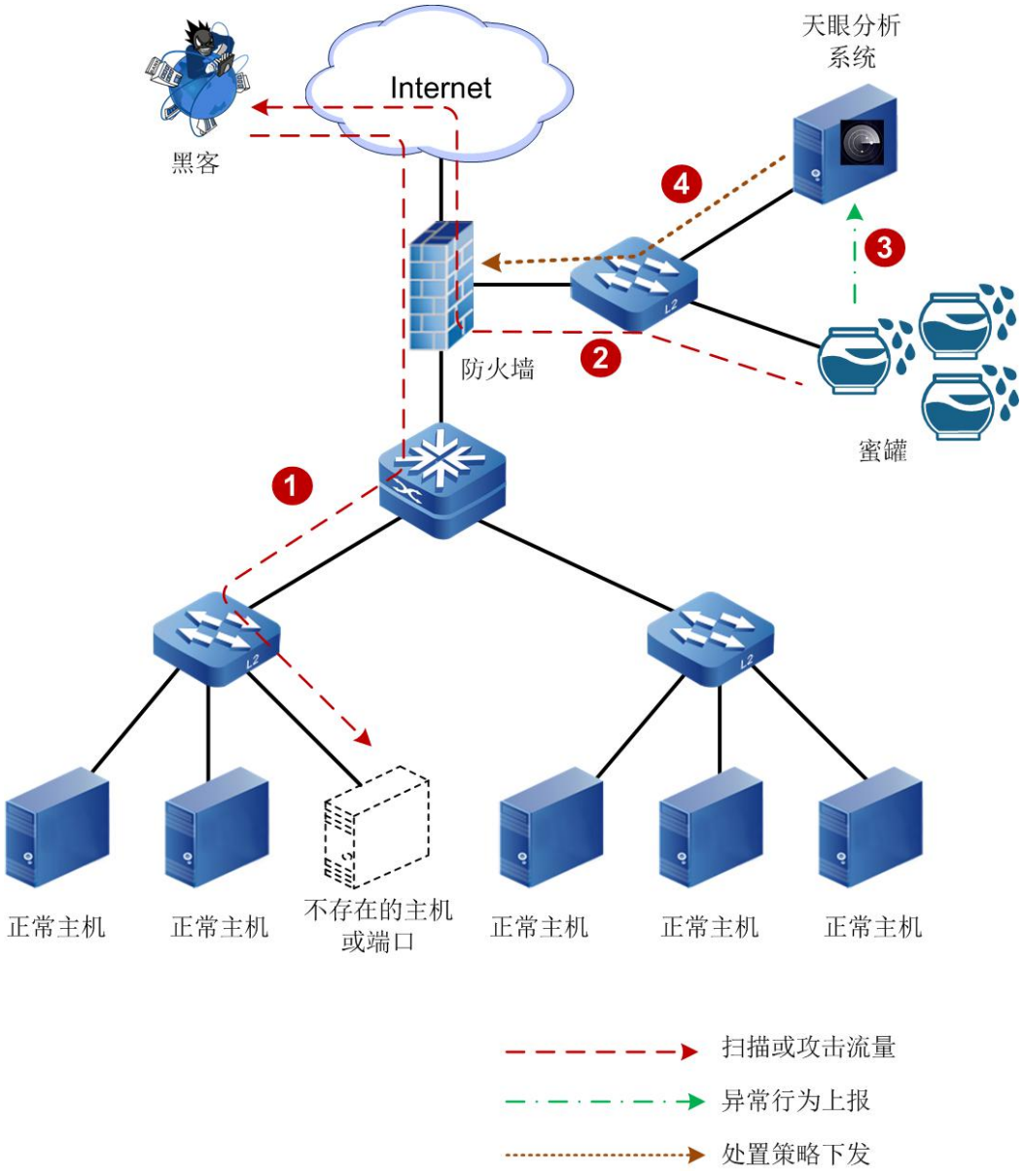
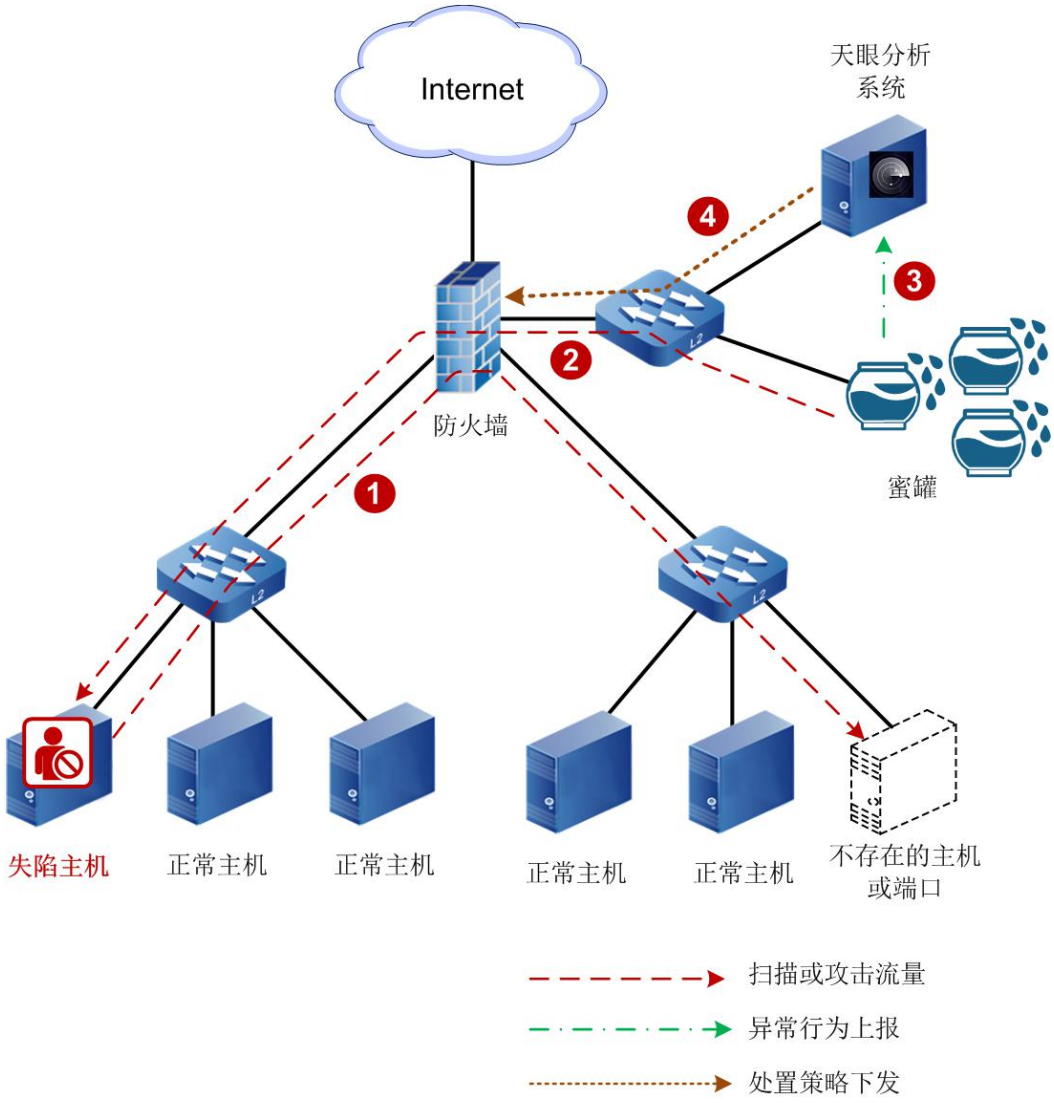


图 2-31 诱捕实现流程-内网



1. 黑客对用户网络进行 IP 地址扫描或 TCP 端口扫描。
2. 防火墙感知到扫描行为后，将可疑流量诱骗至蜜罐进行攻击检测。蜜罐模拟 HTTP/SSH/SMB/RDP 等多种服务，响应黑客的扫描行为，并与其深度互动。分析黑客行为，识别攻击工具，并记录黑客的各种应用层攻击手段和异常行为。
3. 蜜罐将异常行为日志给上报给天眼分析平台。
4. 用户可以在天眼分析平台上对异常行为进行分析。在管理员确认行为异常后，可以在天眼分析平台上下发处置策略给防火墙。
5. 防火墙接收联动处置策略，断开攻击源，保护业务网络。

2.13 应用及流量可视化，网络行为无所遁形

2.13.1 概述

防火墙可以识别 7000+种以上的应用协议，且支持手动添加特定应用，支持深度内容检查技术，无需专业的配置即可识别出应用。

用户需要了解详细的带宽使用情况，可以通过访问防火墙的数据中心实现。数据中心中的日志模块详细记录了用户的上网内容，包括传统的五元组，外加时间、内容、应用、位置和威胁等内容。通过对这些日志的审计和分析，可以对用户的上网流量进行跟踪和分析，了解用户的上网时间、主要访问了哪些网址、使用的是什么应用程序等等。

防火墙支持基于用户的精细化上网流量审计和反查，支持审计的内容如表 2-3 所示。

表 2-3 防火墙审计内容

分类	支持审计的内容
上网流量审计	包括用户访问的目的 IP 地址、目的端口、应用、流量大小等。
DNS 解析审计	主要审计用户进行过的 DNS 解析，包括域名和域名解析后的地址。
即时通讯审计	包括 IM 上下线行为审计，包括上线/下线、IM 号码。
违规内容审计	支持基于关键字进行内容审计，包括用户浏览网页、上传/下载文件、发送/接收邮件等内容里涉及的违规内容审计。
违规文件审计	支持基于文件的过滤和审计，包括用户上传、下载违规格式文件的审计。
恶意行为审计	支持恶意行为的审计，包括攻击、病毒防护、木马防护等。

2.13.2 大容量、多维度日志

防火墙的日志模块支持对用户上网行为和上网内容作多维度详细记录。除传统的五元组外，还记录时间、内容、应用、位置、威胁、安全域等共计 45+个项目和维度，防火墙的安全日志支持本机、Syslog 服务器和第三方管理平台等不同形式存储方式。为日志分析和统计奠定良好基础。

2.13.3 多样化的日志检索方式

防火墙日志模块支持基于关键字的精确筛选和模糊筛选，支持与、或、非、大于、等于、不等于、取反等多样化的过滤条件。支持在日志界面上单击选择，进行快速检索。也支持自定义配置检索条件，同时还支持对检索条件的收藏，方便快速使用。

2.13.4 全方位风险信息展示及分析

防火墙为用户提供了全面的、实时的风险信息展示，着重突出失陷主机、威胁事件、重点关注对象，一键直达异常行为跟踪界面。

防火墙配置威胁分析模块，可通过自定义关键字模糊检索，定位异常行为踪迹，加之对漏洞、应用、会话、网络的全方位监控与分析，确认异常行为是否具有风险。

2.13.5 强大的内容审计策略

防火墙支持强大、灵活的内容审计、文件审计和恶意行为审计策略。

- 内容审计。

系统支持预定义关键字组，包括邮箱、MD5、手机号码、身份证号和银行卡号。同时支持管理员自定义关键字组，管理员可以通过正则表达式匹配或文本匹配的方式，定义需要过滤或审计的关键字。

管理员还可以配置灵活的关键字命中次数，在较宽松的情况下，关键字可以命中多次后，才被记录；在较严格的情况下，命中 1 次即被记录。

- 文件审计

系统支持对指定类型的文件进行管控和审计，包括 html、doc、xls、pdf、rar 等多种文件。系统不基于文件后缀名进行管控，因此，修改文件后缀名的方法无法逃脱防火墙的审计和管控。

系统支持针对于压缩文件的管控和审计，最多可以管控重复压缩 6 次的压缩文件。

- 恶意行为审计

系统支持配置精细化地行为审计策略，包括各种常见攻击、病毒、木马等。

2.14 自动化应急响应功能

防发生紧急网络安全事件时，响应时间窗口直接决定了威胁扩散的范围和资产损失的大小。因此，应急响应是网络安全最重要的一环。

防火墙支持自动化的应急响应功能，该功能针对热点入侵防御事件和威胁情报事件，通过云端下发通知，防火墙自动执行防御的方法，减少由于人为响应和操作带来的时间延迟，从而导致的网络失陷的情况发生。

应急响应时，由天御云统一下发应急响应通知，防火墙收到通知后，自动检测本地的许可证、IPS 库版本和入侵防御策略是否正常。并自动或手动执行防护策略，完成对紧急威胁漏洞的防护。

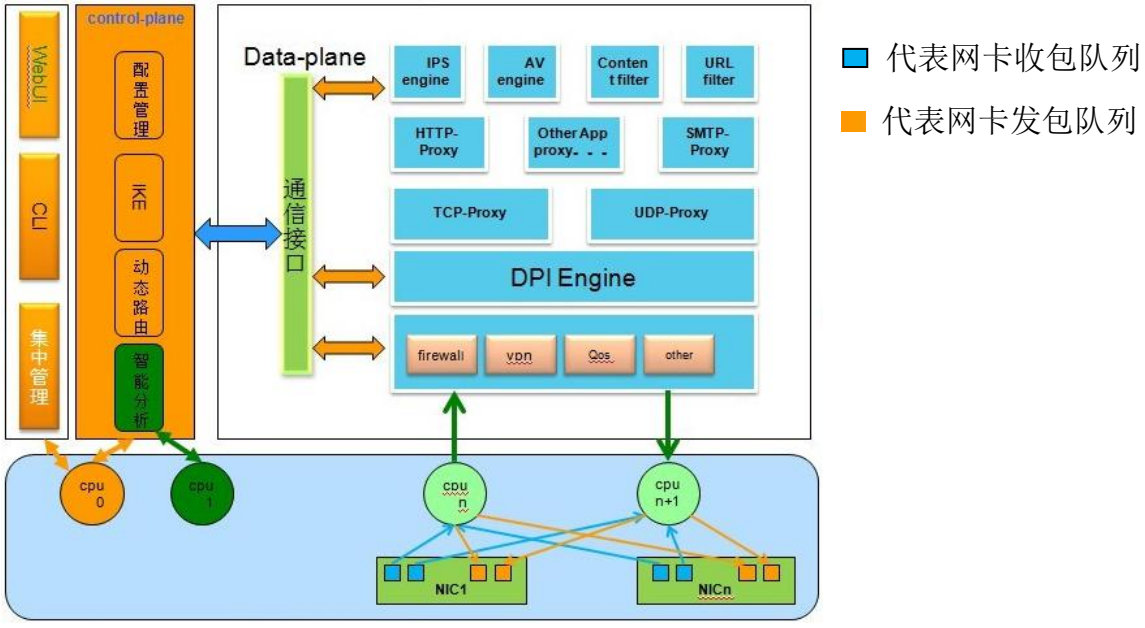
3 技术优势

3.1 采用第四代 SecOS 系统

具备完全自主知识产权的网神第四代 SecOS 操作系统，在第三代 SecOS 带来的高安全性、高开放性、高扩展性和高可移植性基础之上，重点加强了防火墙的协同防御能力、数据生成能力、数据分析能力和数据处置能力，让防火墙具备多端联动、风险信息全方位展示、拦截已知威胁、定位未知威胁和一键处置威胁行为的能力，弥补了传统防火墙重配置轻管理的缺点，并能提供多维度的有效信息帮助用户完成日常维护工作。

3.2 整体框架采用 AMP+并行处理架构

图 3-1 防火墙系统整体框架



防火墙系统的整体框架采用 AMP+架构，是更加优化的多核异步并行处理架构。整体架构分为三大部分：

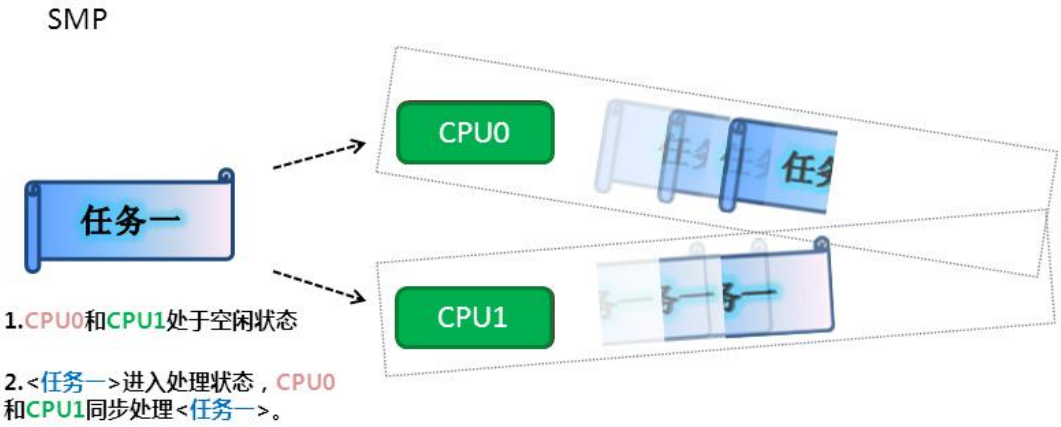
- 配置管理平面：由 CPU0 负责处理。
- 控制平面（control-plane）：由 CPU0 负责处理，其中智能分析功能，由 CPU1 负责处理。
- 数据平面（data-plane）：由剩余的 CPU 平均分配处理。

在 AMP+架构下，多个平面负责各自不同的任务，实现了分层、独立、异步并发的工作体系。为防火墙系统的性能带来了革命性的提升，配置管理平面、控制平面、数据平面的三层分离，保证了防火墙的整体稳定性及可靠性。

3.3 优化的 AMP+架构突破传统 SMP 架构瓶颈

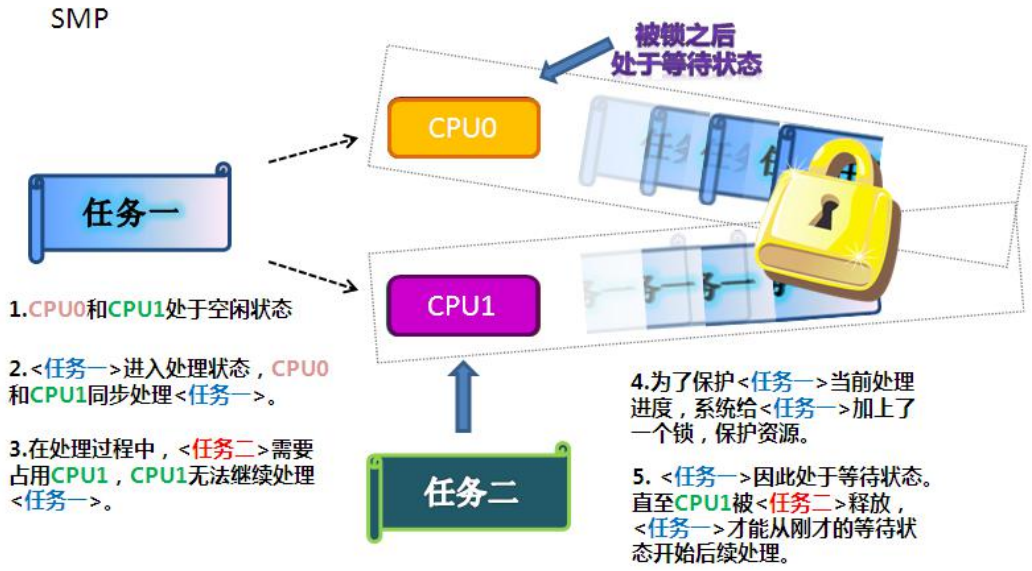
传统的 SMP 架构实现了多核下的并发处理，同一个任务“任务一”分配给了不同的 CPU，如下图所示。

图 3-2 传统 SMP 架构任务处理图 1



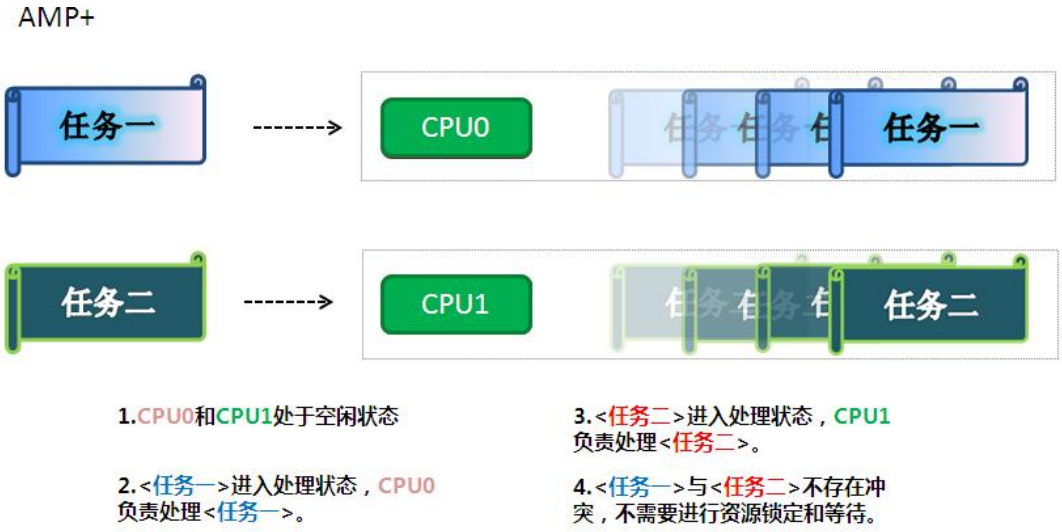
当其中一个 CPU 被其它任务“任务二”占用时，其余正在处理“任务一”的 CPU 就会因为“任务一”被锁而处于等待状态，这就降低了 CPU 的效率，也延长了任务处理时间，如下图所示。

图 3-3 传统 SMP 架构任务处理图 2



防火墙系统采用的 AMP+架构，为异步并行处理架构，不同的 CPU 可以处理不同的任务，这就极大减少了任务被锁住的情况，突破了 SMP 架构下的瓶颈，提升了 CPU 的效率，也极大的缩短了任务处理时间。从而使得防火墙的整体处理速度加快。如下图所示。

图 3-4 防火墙系统 AMP+架构任务处理图



3.4 更优化的网口数据收发处理

以网口数据接收处理为例，传统的多核架构，为了实现多核并行处理，会将CPU 与网口进行绑定。

图 3-5 传统 SMP 架构网口数据处理图



从上图中可以看出，在传统的多核架构下，当网口没有接收到任何数据时，与其绑定的 CPU 就会处于空闲状态，CPU 的利用率并没有实现最大化。

防火墙系统采用的 AMP+架构对此进行了优化，CPU 不再与网口进行绑定，而是由将网卡的收发包队列根据数据平面的 CPU 个数平均分配到每个 CPU 上，这样就保证了数据平面 CPU 的并行度，实现了 CPU 利用率的最大化。

图 3-6 防火墙系统网口数据处理图



从上图中我们可以看出，只要任意一个网口有数据接收，所有的 CPU 就都会处于运行状态，CPU 的利用率到达了最大化。

3.5 单引擎一次性数据处理技术

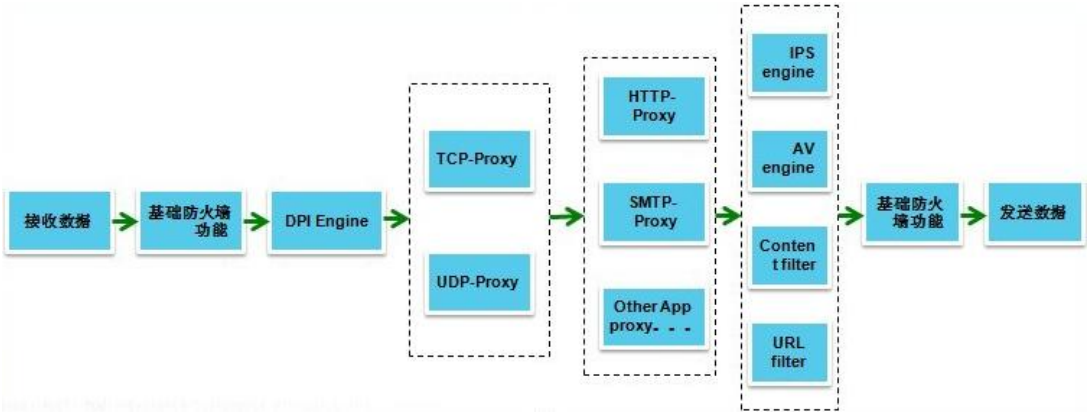
传统防火墙或 UTM 技术大多以 Linux 系统为基础，数据的基本转发功能做在 Linux 系统的内核部分，高级功能（例如 IPS、防病毒、内容过滤等）都做在用户空间，这样就会导致在运行高级防护时，数据需要从内核送到用户空间，处理完后再从用户空间送回内核，然后再发送出去。

这种做法总体有三大缺点：

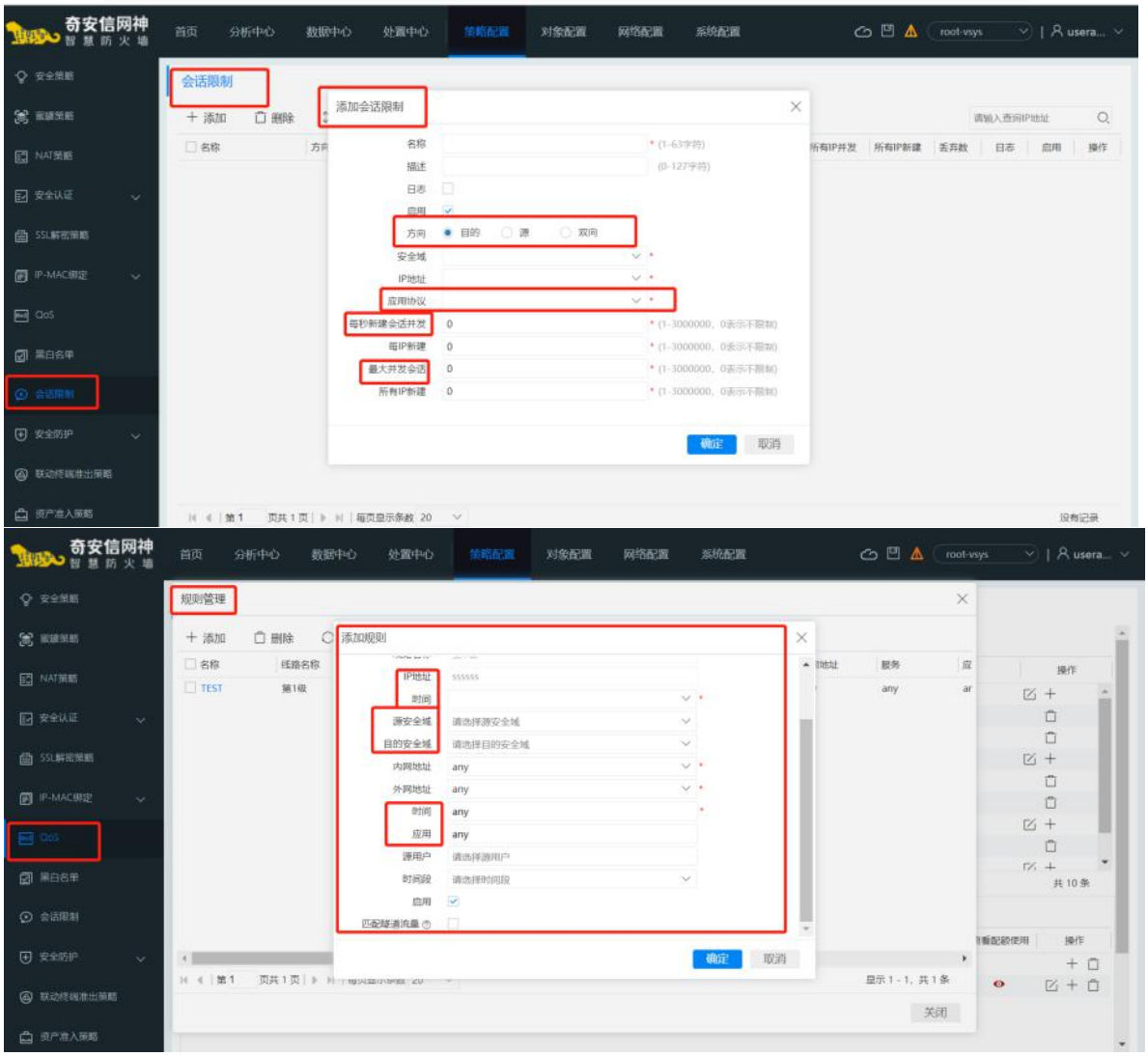
- 涉及到数据包频繁的上下传输。
- 进程间频繁切换
- 会话无法复用

而防火墙系统采用引擎一体化技术后，数据处理流程如下图所示。

图 3-7 防火墙系统单引擎一次性数据处理图



从图中我们可以发现，整个数据的接收、数据的处理（包括应用层数据的处理，IPS、防病毒等高级功能），数据的发送，都在数据平面完成，不涉及数据包的拷贝，进程切换等问题。其会话控制功能，能够基于源、目的、应用协议三种条件做会话数限制，支持针对最大并发会话、每秒新建会话配置限制策略，同时数据的处理在整个转发阶段都使用同一个会话。这就极大的提高了应用层的处理速度，降低了整体数据转发的延迟。同时支持基于安全域、IP 地址、端口、应用、时间等维度设置流控策略，实现多区域流量批量快速管控功能，高效提升访问控制。



3.6 多级冗余架构提高防火墙可靠性

防火墙支持多种多级冗余架构，提升了防火墙的可靠性，包括：

1. 防火墙数据平面冗余架构。由于网口数据的接收和发送任务被平均分配给了每一个 CPU 进行处理，当其中一个或多个 CPU 无法工作时，余下的 CPU 仍然可以正常工作。由于数据的接收和发送任务仍然被平均分配给了每一个当前可以工作的 CPU 上，这就在在数据平面上，提高了防火墙的可靠性。
2. 防火墙系统冗余架构。防火墙支持导入两个系统，并且这两个系统彼此之间是相互独立的。当用户当前正在使用的系统出现问题时，用户可以切换到另一个系统上。这就在系统层面上，提高了防火墙的可靠性。
3. 防火墙网络链路冗余架构。在防火墙系统上，采用增强的 SGRP 路由冗余备份协议，实现双主的路由负载均衡和主备的路由冗余备份两种模式，

同时支持透明环境下的 HA 冗余备份和快速切换。这就在在网络链路上，提高了防火墙的可靠性。

3.7 云端协同扩展精确定位威胁

防火墙除了内置入侵防御、病毒、URL、应用识别特征库外，还可以同天御云进行联动，由云端提供病毒云查杀、URL 云识别、应用云识别、云沙箱等功能。扩展防火墙特征库，精确定位网络中的威胁，并配合处置中心对已确认的威胁行为进行处置。

3.8 基于 NDR 安全体系的未知威胁闭环防御

对于传统安全而言，着重解决了已知威胁，奇安信集团在补充传统安全不足、提升已知威胁识别效率的同时，也思考了未来网络安全发展的新分支。

近几年，信息价值的不断提升，让企业的数据安全面临着更多的威胁及更深的影响，传统安全手段解决已知威胁的方式并不能真正保护用户的数据安全。高级威胁往往可以透过合规数据绕过传统安全的各种防御手段并成功达到数据窃取的目的。因此，我们迫切需要一个新的安全体系来对未知威胁进行防范与跟踪。结合奇安信大数据挖掘技术及数据安全分析中的积累，奇安信集团建立了由大数据驱动，基于网络的检测与响应体系（简称 NDR）。针对未知威胁形成一套基于互联网及用户自身网络的动态数据检测、动态行为检测、动态处置响应的防御闭环。

图 3-8 基于 NDR 安全体系的未知威胁闭环防御

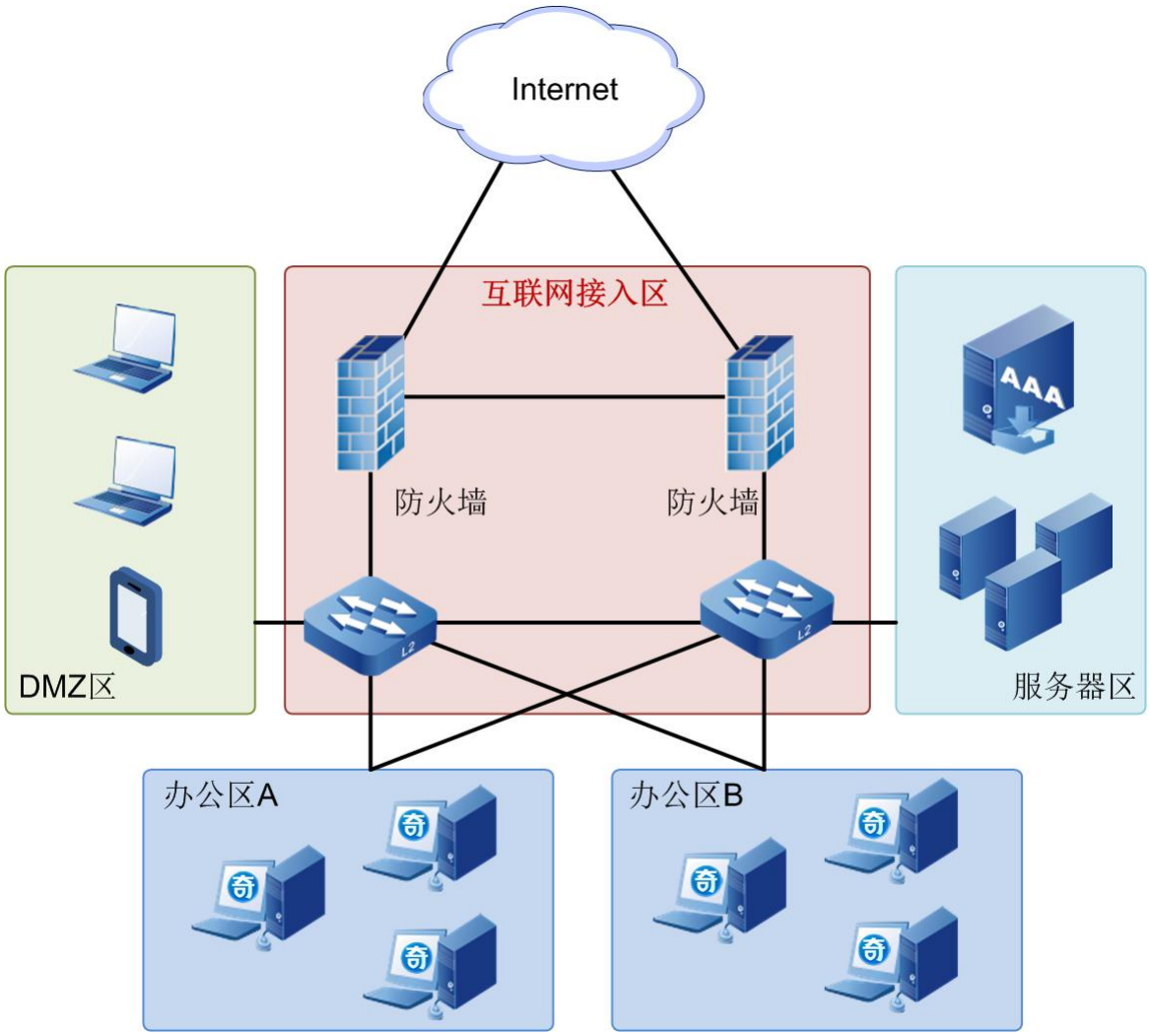


防火墙系统作为 NDR 安全体系中的重要一环，利用对用户自身网络的数据识别、行为识别，加之云端基于特征的已知威胁、基于沙箱的未知威胁检测、基于威胁情报的失陷主机发现、基于安全模型的未知威胁发现，结合防火墙/SMAC 的多维度关联分析、递进式数据钻取，直观展现未知威胁行为的跟踪、定位、处置，完成对未知威胁的一键式处置及策略优化，及安全事件的溯源取证。

4 应用场景

4.1 企业互联网边界安全应用场景

4.1.1 典型场景

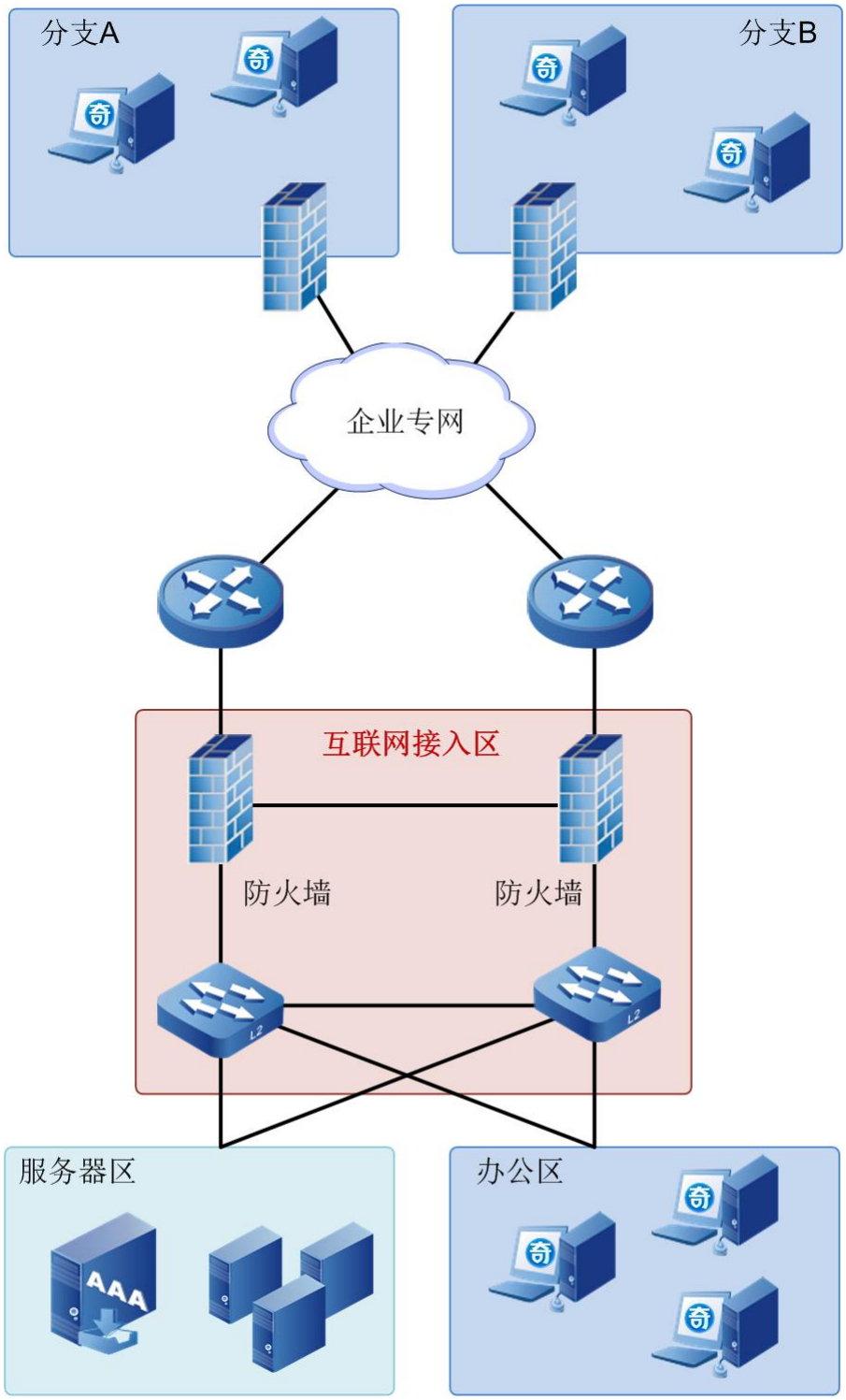


4.1.2 痛点和优势

痛点	优势
外部威胁多，上网用户网络安全意识参差有别	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
内部网络流量成分复杂	全面健壮的应用层级综合安全防护
重点业务保证，需对上网的带宽及行为进行约束	按需动态调整带宽

4.2 行业专网网络安全应用场景

4.2.1 典型场景

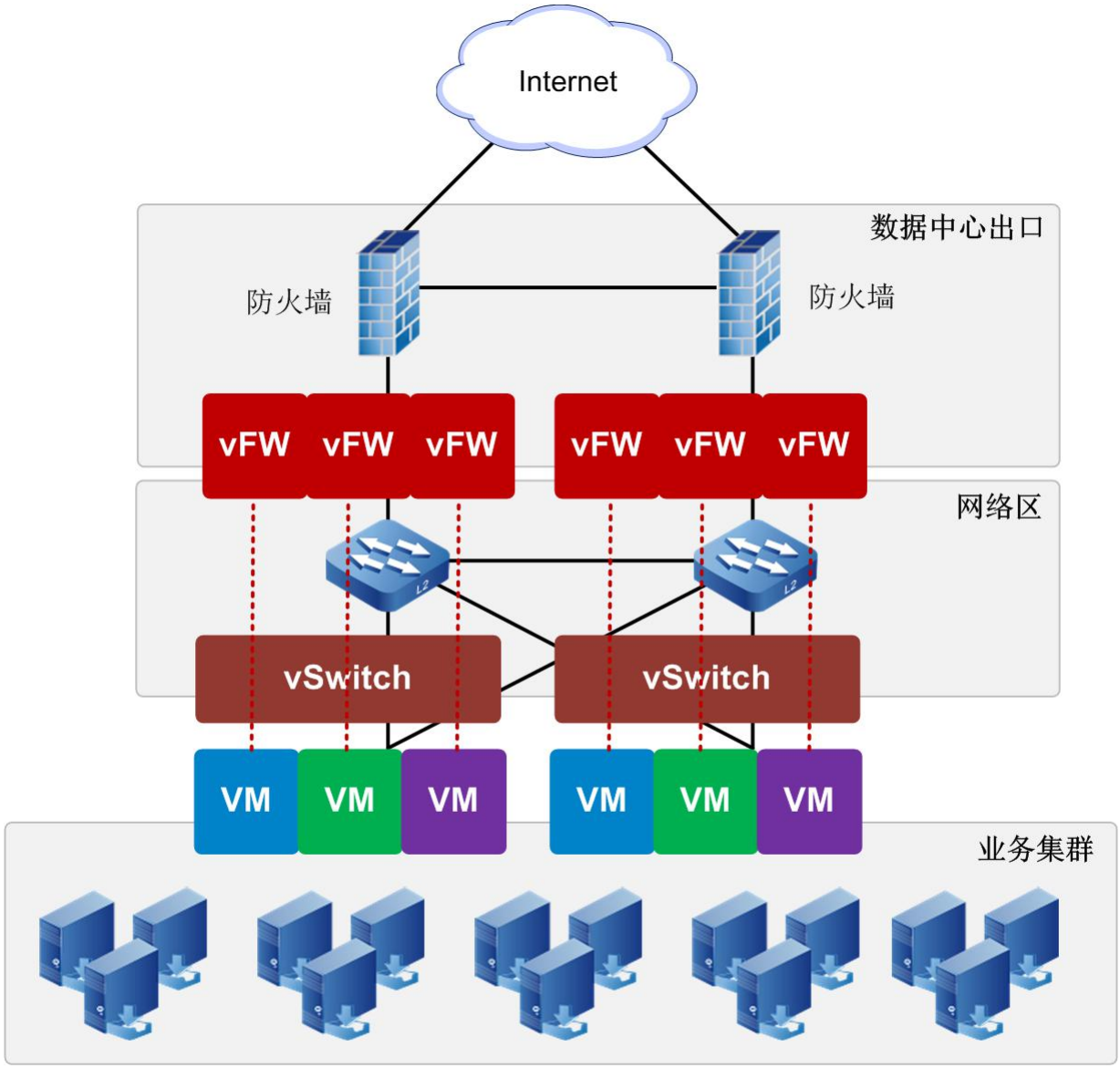


4.2.2 痛点和优势

痛点	优势
多链路备份，提升网络可用性	高效的双机热备
多分支互联，业务安全传输	标准的 IPSec VPN、SSL VPN 功能
重点业务保证，需对上网的带宽及行为进行约束	按需动态调整带宽
内部网络流量成分复杂	全面健壮的应用层级综合安全防护
外部威胁多，上网用户网络安全意识参差有别	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

4.3 数据中心出口安全应用场景

4.3.1 典型场景



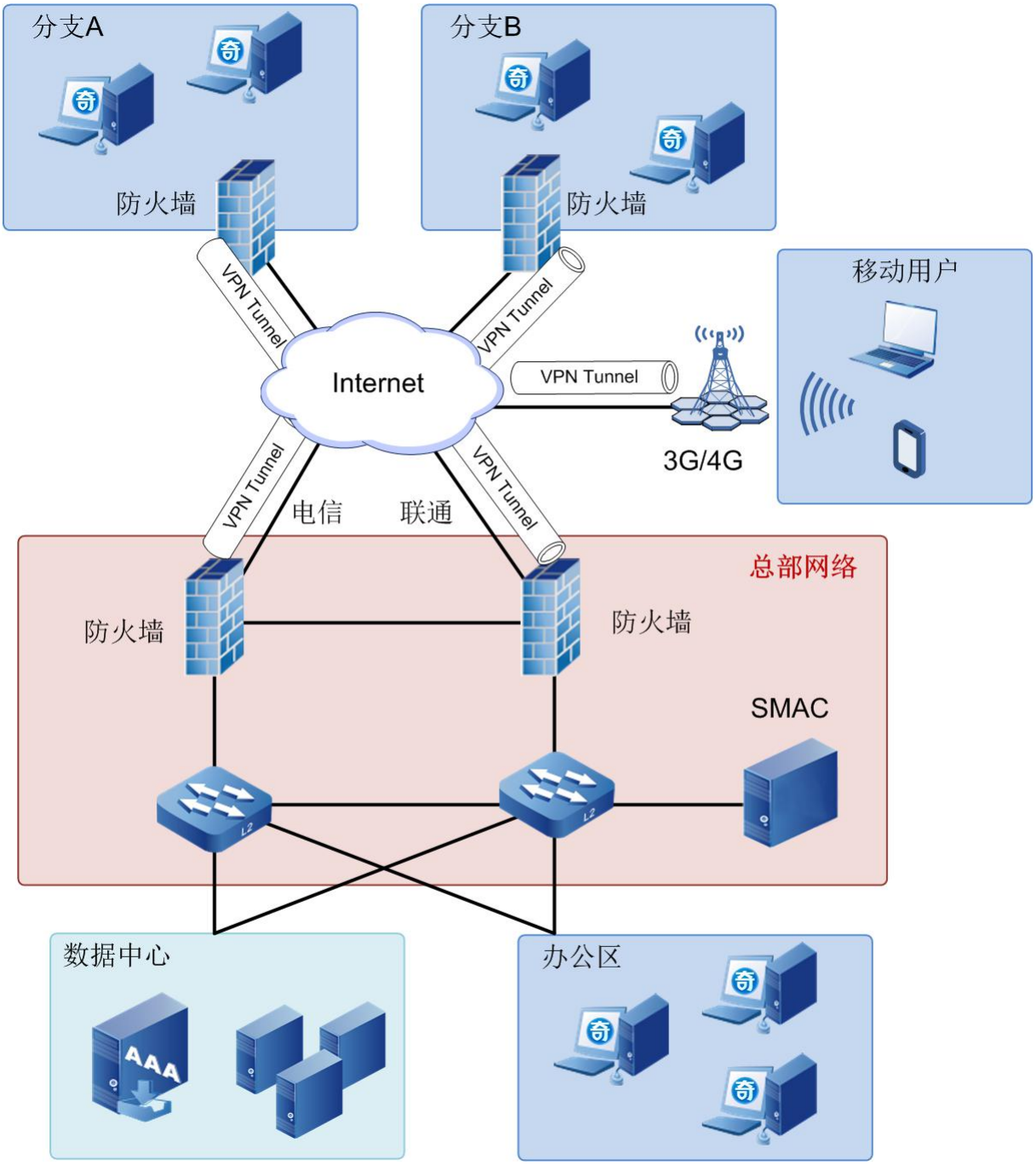
4.3.2 痛点和优势

痛点	优势
出口大流量承载	高性能承载出口大流量
全网可靠性要求高	全网冗余设计保证可靠性

痛点	优势
全网安全性要求高	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
业务众多且网络复杂度高	虚拟防火墙承载业务实现安全隔离
需对业务实现安全隔离与管理	独立配置、独立分析、独立维护

4.4 多分支企业组网安全应用场景

4.4.1 典型场景



4.4.2 痛点和优势

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