

应用防火墙

DPtech FW1000 系列防火墙技术白皮书

1、概述

在应用需求的不断推动下，网络技术得到了飞速发展；而网络技术的进步则又反过来推动应用的发展，应用与网络之间是相辅相成、相互促进的。随着万兆到核心/千兆到桌面、Web2.0、虚拟化、物联网、网络音频/视频、P2P、云计算等各种新应用、新业务层出不穷，传统的基于端口进行应用识别和访问控制的防火墙，已远远无法满足各种新应用下安全防护的需求。为解决此类难题，迪普科技推出了基于全新多核处理器架构的 FW1000 系列下一代应用防火墙。

DPtech FW1000 开创了应用防火墙的先河。基于迪普科技自主知识产权的 APP-X 硬件平台和 ConPlat OS 安全操作系统，并配备专业的入侵防御特征库、病毒库、应用协议库、URL 库，是目前业界性能领先的应用防火墙。无以伦比的高可用性、高性能和高可靠性，使得 FW1000 系列可以放心规模部署于数据中心、大型园区网等各种复杂场景；另外，功能丰富并可按需扩展的应用防火墙方案，也简化了网络的安全架构，并大大降低了企业网络总体拥有成本。



2、产品简介

DPtech FW1000 系列是迪普公司面向大中型企业、学校、数据中心以及运营商开发的新一代应用防火墙产品，是一种应用级的高性能防火墙，工作在网络边界层，根据安全策略对来自不同区域的数据进行安全控制，同时支持 IPv4 和 IPv6 环境，具备高性能，网络无瓶颈，拥有全面的安全防护，可确保网络稳定运行，产品 VPN 全内置，提供高性价比，灵活组网能力，可适应各种网络环境。

3、迪普科技防火墙特色技术

3.1 DPtech FW1000 防火墙数据转发流程

防火墙的用途是通过允许、拒绝、重定向通过防火墙的数据量，提供对一个组织的不同网络之间服务访问的控制和审计，包括基于用户和协议的策略定义、URL 过滤、协议识别等特性，DPtech FW1000 防火墙设备同时支持包过滤和应用级防火墙要求。

防火墙根据网络中各点的安全规则策略，有选择的在不同网络间发送信息流，默认安全规则策略拒绝所有入站和出站的信息流，仅授权的管理员具有改变安全规则策略的权限。典型的包过滤策略由源地址、目的地址、传输层协议、源端口、目的端口、应用协议决定，并以数据包达到或者离开接口为基准。

迪普防火墙采用安全域的控制方式在包过滤处进行整体调用，默认规则为：

- 1、高安全域可以访问低安全域。
- 2、低安全域不可访问高安全域。
- 3、相同安全级别的不同安全域，相互间禁止访问。
- 4、同一个安全域下面的不同接口，接口间可相互访问。

防火墙内部数据转发简要流程图如下：

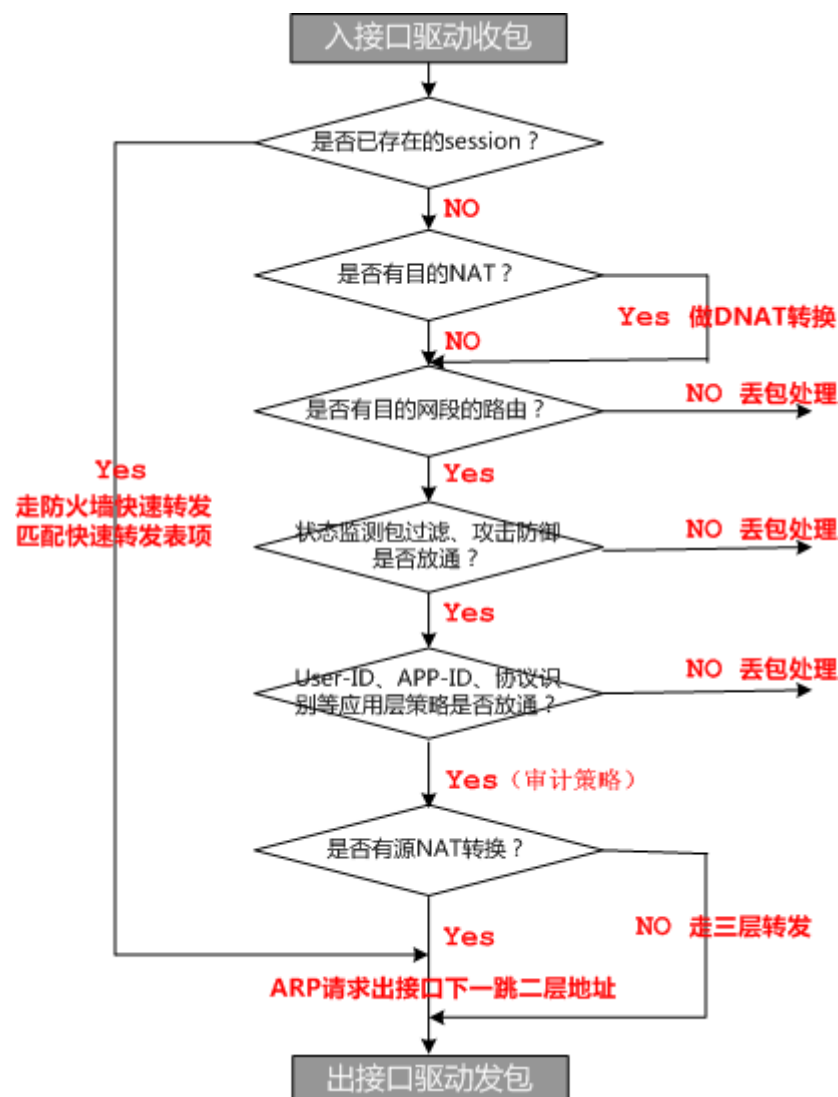


图 1 防火墙内部转发流程图

防火墙数据转发流程依据上述顺序进行，先查找会话表项，然后再目的 NAT 转换，路由查找，包过滤规则，防火墙策略、应用层匹配规则，审计策略，最后查询源 NAT 从设备转发出去。

3.2 丰富的网络特性

ConPlat 软件平台支持丰富的网络特性，既包括 STP、VLAN、ARP 等二层特性、也包括 BGP、OSPFv2/v3、MPLS 等 IPv4/IPv6 的三层特性。

DPtech FW1000 网络特性：

- 支持透明组网模式、路由组网模式、旁路组网模式、混合组网模式
- 支持 IPv4/IPv6 协议栈，具备完善丰富的 IPv6 协议栈过渡以及隧道技术
- Access、Trunk VLAN、端口聚合、端口镜像
- 策略路由、静态路由、组播 IPv4/6 路由(IGMP、PIM、MSDP、组播 VPN)
- IPv4 路由（支持 RIP v1/2、OSPF、IS-IS、BGP、Guard 路由）
- IPv6 路由（支持 RIPng、OSPFv3、Guard 路由）、IPv6 隧道技术
- 支持完善的 MPLS VPN
- 支持 DNS、DHCP、ARP、BFD、STP、QOS
- 支持链路负载、链路调度、会话保持、DNS透明代理

迪普防火墙丰富的网络特性为用户提供了灵活组网能力，可适应各种类型的网络环境，支持路由模式、透明模式、旁路模式、混合模式组网，可适应各种复杂应用组网环境。

3.3 海量策略数下的高性能、低时延处理能力

迪普防火墙包过滤、NAT 匹配采用决策树算法把安全策略编译成快速匹配表项，报文经过设备时提取五元组一次性送入快速匹配表项进行策略匹配，可以一次性查找到相应的匹配，形成单数据流并行处理的体系结构，即便防火墙在有海量策略数的情况下，依旧可保持高性能、低时延的处理能力，满足管理员对设备超高处理性能与低传输延迟的需求，让安全防护设备从此不再成为网络传输的瓶颈。

3.4 攻击防范技术 (IPv4/IPv6)

攻击防范功能是 DPtech 防火墙的重要特性之一，是指通过分析报文的内容特征和行为特征判断报文是否具有攻击特性，并且对攻击行为采取措施以保护网络主机或者网络设备。

防火墙的攻击防范功能能够检测拒绝服务型（Denial of Service, DoS）、扫描窥探型、畸形报文型等多种类型的攻击，并对攻击采取合理的防范措施。攻击防范的具体功能包括黑名单过滤、报文攻击特征识别、流量异常检测和入侵检测统计。

除了对传统的 IPv4 安全防范技术，迪普防火墙对于 IPv6 的安全也拥有全面防护，支持 IPv6 的包过滤、业务长连接、huge-icmp-pak、icmp-flood、ip-sweep、ip-spoofing (I2/I3)、udp-flood、tear-drop、ip-fragment、ping-of-death、port-scan、syn-flood、syn-proxy、tcp abnormal、land-attack、NDP defender 等。

■ DDoS 攻击

在多种网络攻击类型中，DDoS 攻击是最常见的一种，因为这种攻击方式对攻击技能要求不高，攻击者可以利用各种开放的攻击软件实施攻击行为，使用大量的数据包攻击目标系统，让目标系统无法接受正常用户的请求，或者使目标主机挂起不能正常工作。DDoS 攻击和其它类型的攻击不同之处在于，攻击者并不是去寻找进入目标网络的入口，而是通过扰乱目标网络的正常工作来阻止合法用户访问网络资源。

防火墙通过攻击防范技术可主动防御各种常见的网络攻击，保证网络在遭受越来越频繁的攻击的情况下能够正常运行，从而实现防火墙的整体安全防护。对于采用服务器允许的合法协议发起的 DDoS 攻击，攻击防范采用基于行为模式的异常检测算法，能够精确识别攻击流量和正常流量，有效阻断攻击流量，同时保证正常流量通过，避免对正常流量产生拒绝服务。攻击防范能够检测到的流量异常攻击类型包括 SYN Flood、ICMP Flood、UDP Flood 等。

DDoS 攻击也可以存在于 IPv6 Internet 上。由感染木马的计算机组成的大型网络成为僵尸网络，他们的攻击可以聚焦到一个受害者。IPv6 的使用不会改变僵尸网络的生成和运行，不幸的是，僵尸网络将仍然存在于 IPv6 网络上。IPv6 将允许 Internet 包含比 IPv4 Internet 更多的设备，如果这样多的设备都发起一次 DDoS 攻击的情形，相比如今在 IPv4 Internet 上的攻击而言，结果将更具毁灭性。

迪普防火墙支持 DDoS 指纹识别技术，可针对网络中的 IPv4/IPv6 流量进行自动学习，形成用户流量指纹特征，如果网络有攻击出现异常攻击流量，DDoS 将快速识别异常流量，阻断攻击流量或者对攻击流量进行限速处理，实现 DDoS 攻击防御的智能化、简洁化。同时用户还可以手动配置指纹识别的特征，对特定的流量进行识别，如 TCP 可配置参数有报文长度、报文 ID、TTL、源 IP、目的 IP、序列号、确认号、源端口、目的端口、flag 标记以及自定义特征，可对于已知的攻击特征可进行有效手动识别与防护。

■ 扫描窥探攻击

扫描窥探攻击利用 PING 扫描（包括 ICMP 和 TCP）标识网络上存在的活动主机，从而可以准确地定位潜在目标的位置；利用 TCP 和 UDP 端口扫描检测出目标操作系统和启用的服务类型。攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入目标系统做好准备。迪普防火墙能够有效的防御 IP 地址扫描、端口扫描、漏洞扫描等扫描窥探攻击。

■ 畸形报文攻击

畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这样的 IP 报文时崩溃，给目标系统带来损失。迪普防火墙通过特征识别技术，能够精确识别出数十种攻击特征报文，能够对 LAND 攻击、死亡之 Ping、IP 分片重叠攻击、UDP Fraggle 攻击、WinNuke 攻击、TcpFlag 攻击、ICMP 不可达报文、ICMP 重定向报文、ICMP Smurf 攻击、源路由选项 IP 报文、路由记录选项 IP 报文、超大 ICMP 报文等畸形报文攻击进行防护。

3.5 病毒过滤技术

通过集成专业病毒特征库向用户提供防病毒服务，能够检测 HTTP、FTP、SMTP、POP3、IMAP、RAR、ZIP 等传输的病毒。防病毒模块可以以在线、旁路、桥接和混合等模式部署在网络中，通过采用实时分析的方式，自动检测、阻断或重定向携带病毒的报文与异常流量。防病毒模块提供的功能包括：

- 防病毒规则管理

- 防病毒特征查询

防病毒日志

支持防御文件型、网络型和混合型等各类病毒，能够通过新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒。设定三种级别流行性病毒检测，根据流行度，用户可以配置开启不同级别的病毒防护控制。防病毒特征库定期更新以保证对新病毒的及时响应。防病毒模块的基本功能和原理，如下图所示。

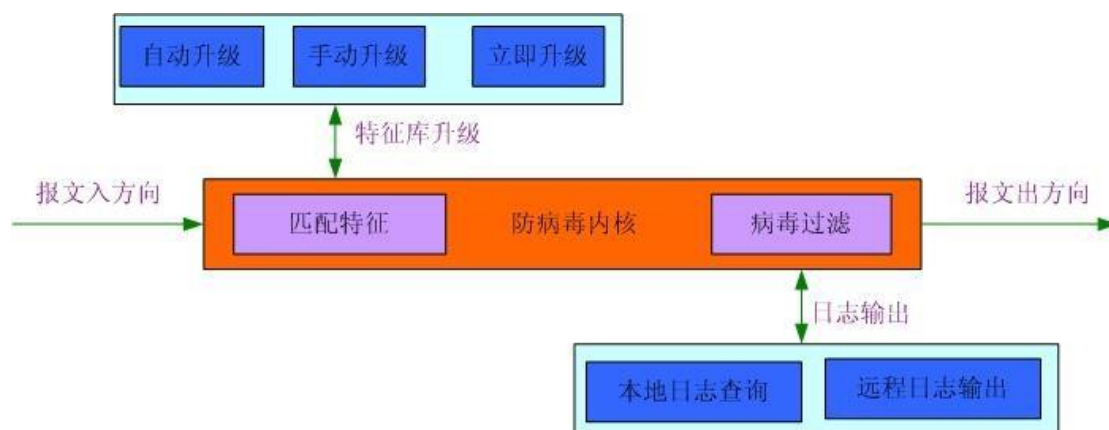


图 7 病毒检测与防护

传统的检测病毒的方法，可以分为四种：特征代码法，校验和法，行为检测法，和软件模拟法。在网络设备上实现防病毒功能，最好的方法就是特征代码法。通过集成专业病毒库，精确扫描经过设备的网络数据流，如果与特征相符，就认定为病毒。不同的病毒特征，划分病毒的流行度，可以有不同的防护动作，并生成日志。迪普科技防病毒查杀具有：检测准确快速、可识别病毒的名称、误报警率低等优点。

迪普科技的防病毒日志有丰富的报表功能，能提供各种查询条件，如病毒源 IP，目的 IP，病毒种类，各个时间段等等。日志支持远程发送，也支持日志备份等操作。迪普科技 IPS 病毒库以定期（每周）和紧急（当重大安全病毒特征被发现）两种方式发布，并且能够自动分发到用户驻地的设备中。

3.6 Web应用防护

- 参数攻击防护 支持Sql注入攻击防护，Xss攻击防护、命令注入防护、目录遍历攻击防护等
- HTTP协议攻击防护 支持对HTTP协议请求正规化检查，Cookie正规化检查，Cookie加密等
- 支持缓冲区溢出攻击防护、弱口令、暴力破解、爬虫、盗链等防护功能

3.7 防火墙高可靠性

DPtech FW1000 具备完善的双机热备技术，包括普通双机热备、高级双机热备、非对称双机热备、静默双机热备等。

■ 普通双机热备

提供配置同步的双机功能，实时相互备份防火墙的配置，包括 IP 地址对象/组、服务对象/组、包过滤策略、路由等。

■ 高级双机热备

在提供备份配置的基础上，实时同步两台防火墙的会话，一旦主备发生切换，有状态连接的应用访问可继续进行，无需重新连接。

■ 非对称双机热备

可配置备份与会话备份，同时支持业务流量非对称的双主部署模式。对于 ALG 的会话实时同步，对多通道应用层业务提供支持。

普通、高级以及非对称双机热备主备切换可配合协议来实现，如 VRRP 协议、OSPF 协议、STP 协议等。管理员通过规划 VRRP、OSPF、STP 等的优先级参数来控制业务流量走向，从而实现防火墙部署为主备模式或主主模式，如下图：

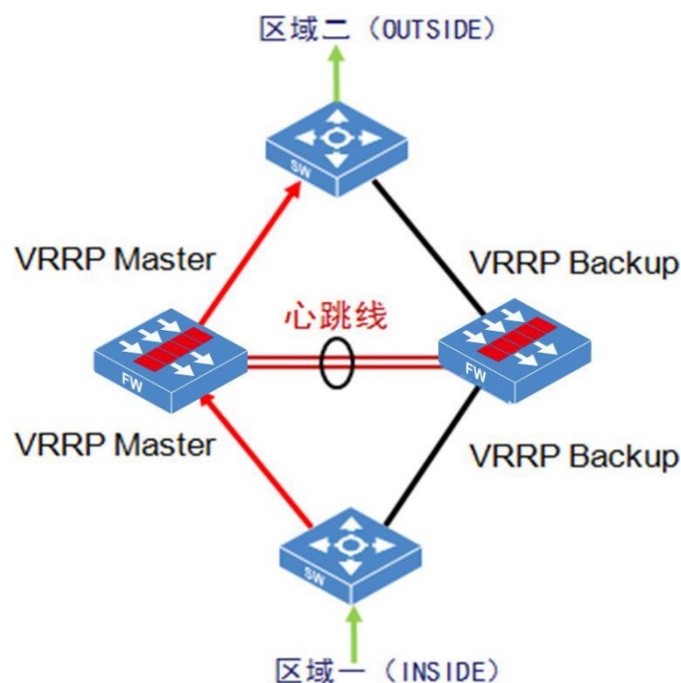


图 2 双机热备 (VRRP 协议)

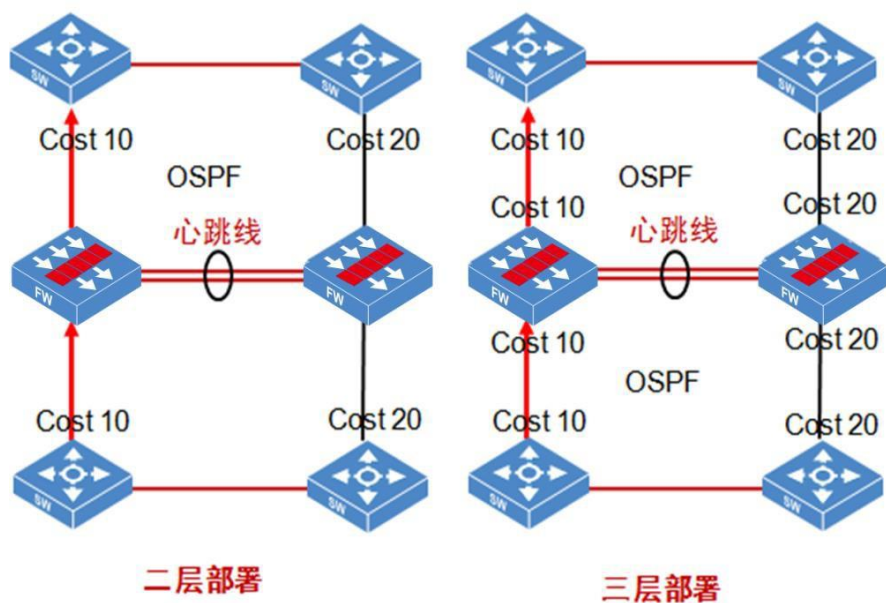


图 3 双机热备 (OSPF 协议)

■ 静默双机热备

主备防火墙所有配置完全一样（接口 IP 也一致），正常运行的情况下，逻辑上只能感知到主设备的存在，备设备处于静默的状态，在网络中不可见也不可感知。主设备通过心跳线定时的发送自己的心跳报文用来通告自己的运行状态。备设备只监听主设备的状态，不发包也不收包，处于静默的状态。

当主设备有异常，或备设备在一定时间段之内没有收到主设备的心跳报文，那么备设备就会 Wake Up，变成主防火墙，通过连续发送免费 ARP 的机制，不断刷新交换机上的 MAC 地址表项，将业务流量牵引过来接替主设备进行转发。从而实现流量双机热备。这种方式不需要借助其他的协议实现，而是通过设备自身检测机制来实现双机热备，相对简单可靠。

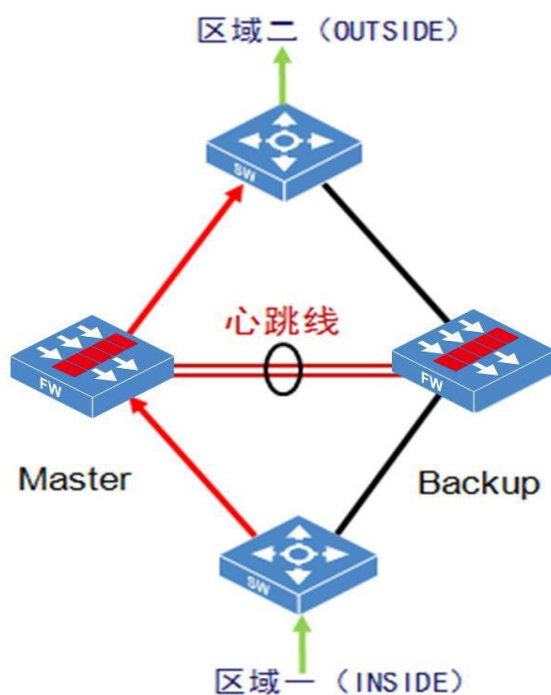


图 4 静默双机热备

3.8 防火墙全面 VPN 支持

DPtech FW1000 面对用户分支互联、移动办公的需求，支持丰富的 VPN 种类，包括 IPSec、SSL、GRE、L2TP、PPTP 等多种 VPN 接入方式，并提供包括 DES、3DES 等多种加密算法，并支持证书认证。防火墙内置 IPSec VPN、SSL VPN 高速硬件加密功能，在简化网络结构的基础上，还大大提升了用户网络安全建设的性价比。

√ Site to Site 固定接入类型

- IPSEC VPN
- GRE VPN



图 5 Site to Site VPN 接入

√ 移动接入类型

- IPSEC VPN
- PPTP VPN
- L2TP VPN
- SSL VPN

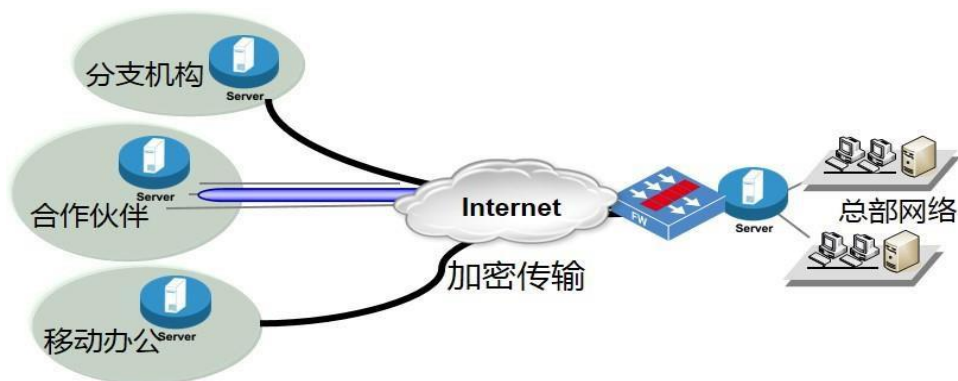


图 6 移动办公 VPN

3.9 防火墙虚拟化技术

3.8.1 虚拟防火墙技术

DPtechConPlat 平台支持操作系统级或应用级的虚拟化特性。所谓操作系统级虚拟化是服务器虚拟化中的一个概念，指的是在主操作系统上运行一个虚拟层软件，可以安装多种客户操作系统，任何一个客户系统的故障不影响其他用户的操作系统。通过安装于主操作系统（Host OS）之上的虚拟化软件将 Guest

OS 的内核和文件系统抽象化为一个个容器，并负责计算存储源分配及容器安全隔离。ConPlat 操作系统级虚拟化如下图所示：

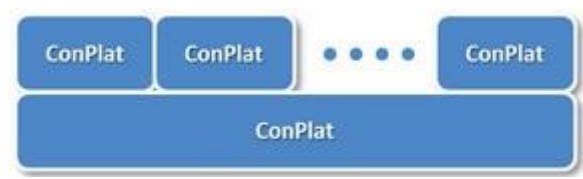


图 7 操作系统级虚拟化

所谓应用级虚拟化，指的是在单一操作系统上使用，在操作系统和应用之间运行虚拟层，任何一个应用包的故障不影响其他软件包。应用级虚拟化可以将 ConPlat 的核心功能打包成为一个虚拟防火墙，每个虚拟设备都有独立的计算资源、转发表项、控制平面、业务平面及转发平面进程，以及独立的管理员与管理界面。ConPlat 应用级虚拟化如下图所示：



图 8 应用级虚拟化

操作系统级虚拟化与应用级虚拟化的区别在于完整程度。进行操作系统级虚拟化后，每个虚拟化实例依然是一个完整的 ConPlat 软件平台，在其上依然可以进行应用级虚拟化，如进一步划分虚拟防火墙。而应用级虚拟化只是将 ConPlat 的核心功能虚拟化成为一个虚拟设备，每个虚拟化实例并不是一个完整的 ConPlat 软件平台，并不能将这些虚拟设备进一步的虚拟化。

传统防火墙是一个物理的实体，而虚拟防火墙是在这个物理实体里面划分出来的多个虚拟的防火墙。虚拟防火墙的功能是原防火墙的一个子集。虚拟防火墙多部署在运营商或者 IDC 机房的网络中，由运营商购买并维护物理防火墙实体，用户可以租用一个或多个虚拟防火墙，并管理属于自己的那部分资源。

虚拟防火墙之间完全隔离，每个虚拟防火墙有自己独立的用户管理系统，可以管理属于自己的硬件接口等硬件资源，也可以管理分配给自己的安全域、VLAN 等逻辑资源。

■ 管理员的虚拟化

管理员	登录时间	最近访问时间	登录地址	操作
admin	2011-09-14 19:14:00	2011-09-14 19:19:34	10.11.0.7	
admin	2011-09-14 19:08:48	2011-09-14 19:15:56	10.11.12.155	🔍
admin	2011-09-14 18:59:30	2011-09-14 19:15:13	10.11.12.155	🔍

管理员设置

管理员	密码	确认密码	描述	虚拟系统	配置范围	配置权限	状态	操作
admin	*****	*****		公共系统	Super	1(最高)	正常	🔍
xiaohaibo	*****	*****		qq	Super	1(最高)	正常	🔍 ✖
				公共系统				
				qq				
				aa				

图 9 防火墙管理员虚拟化

每个虚拟系统都有自己独立的管理员。公共系统为全局系统，可以管理设备上所有的管理员。虚拟系统的管理员只能看到并管理属于这个虚拟系统的管理员。

物理硬件资源的虚拟化

虚拟系统配置

名称	接口	操作
公共系统	vlan-if1, vlan-if8, vlan-if9, vlan-if10, eth0_4, eth0_5, eth0_6, eth0_7,	🔍
qq	vlan-if2, vlan-if3, vlan-if4, eth0_0, eth0_1,	🔍 ✖
aa	vlan-if5, vlan-if6, vlan-if7, eth0_2, eth0_3,	🔍 ✖

图 10 防火墙物理资源虚拟化

每个虚拟系统都分配了属于自己的接口，每个虚拟系统的管理员可以为自己的接口划分 VLAN、设置 IP 等。

逻辑资源的虚拟化

VLAN配置

批量添加VLAN		批量删除VLAN				浏览...		导入		导出	
共：10条数据										第 1 / 1 页 每页 25 条	
VLAN ID	名称	虚拟系统	描述	类型	包含端口	操作					
1	VLAN1	公共系统	无	静态	无						
2	VLAN2	qq	无	静态	无	✖					
3	VLAN3	qq	无	静态	无	✖					
4	VLAN4	qq	无	静态	无	✖					
5	VLAN5	aa	无	静态	无	✖					
6	VLAN6	aa	无	静态	无	✖					
7	VLAN7	aa	无	静态	无	✖					
8	VLAN8	公共系统	无	静态	无	✖					
9	VLAN9	公共系统	无	静态	无	✖					
10	VLAN10	公共系统	无	静态	无	✖					
共：10条数据										第 1 / 1 页 每页 25 条	

图 11 Vlan-if 虚拟化

对于 VLAN 这种全局统一的逻辑资源，由公共系统的管理员统一创建，然后分配给不同的虚拟系统。各虚拟系统的管理员可以为自己的 VLAN 配置 IP、把接口划分到自己的 VLAN。



序号	安全域名	虚拟系统	接口	优先级[0-100]	描述[可选]	操作
1	trust	qq	eth0_4	1	无	 
2	untrust	qq	eth0_1	1	无	 

图 12 安全域虚拟化

对于安全域这种纯软件的逻辑资源，由各虚拟系统的管理员自己维护。

■ 路由虚拟化

路由虚拟化分为两个层次，一个是转发层面的虚拟化，一个是路由管理的虚拟化。从内核态转发层次看，每个虚拟防火墙包含多个硬件接口。这些硬件接口由自己的虚拟转发平面管理，不同的虚拟防火墙之间完全隔离。因此，不同的虚拟防火墙配置相同的 IP 地址是允许的。

请选择VRF ID：




VRF_0

系统配置：

☒ 启动OSPF

高级配置

区域配置：

区域ID	使能接口	高级配置	操作
请配置	请配置		 

接口配置：

接口名	Hello间隔	Dead间隔	认证信息	高级配置
eth0_0	10	40	无	cost自动 / 优先级:1 / 工作模式:活跃 / 类型:broadcast
eth0_1	10	40	无	cost自动 / 优先级:1 / 工作模式:活跃 / 类型:broadcast
eth0_2	10	40	无	cost自动 / 优先级:1 / 工作模式:活跃 / 类型:broadcast
eth0_3	10	40	无	cost自动 / 优先级:1 / 工作模式:活跃 / 类型:broadcast
eth0_4	10	40	无	cost自动 / 优先级:1 / 工作模式:活跃 / 类型:broadcast

图 13 路由虚拟化

从用户态路由管理层次看，每个虚拟系统有自己的路由管理软件，不同的虚拟系统有自己独立的管理域，拥有独立于其他虚拟系统的管理进程，使 OSPF、BGP 等路由程序可以独立运行、独立管理。因为虚拟系统的管理域是独立的，因此虚拟系统之间可以更合理的分配 CPU 资源，而且一个虚拟系统的崩溃不会影响其他的虚拟系统。

3.8.2 VSM 虚拟化技术

从提出虚拟化理念开始，虚拟化技术在不断发展、变化中，不同厂商的技术实现也不尽相同。迪普科技推出了业界首创的网络及应用一体化的虚拟化技术 - VSM（Virtual Switching Matrix 虚拟交换矩阵）。



图 14 VSM 多框级联

多个 VSM 成员设备之间使用多个 10G 口聚合，VSM 系统和上、下层设备之间的连接也使用聚合相接，这样通过多链路备份提高了 VSM 系统的可靠性同时保障了网络逻辑链路的简洁性。VSM 系统由多台成员设备组成，Master 设备负责 VSM 的运行、管理和维护，Slave 设备在作为备份的同时也可以处理业务，一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证通过 VSM 的业务不中断，从而实现了设备级的 1:N 备份。

VSM 可以支持扩展的 SW、FW、IPS、UAG、ADX、SSL VPN 等功能板卡，轻松扩展网络接口、功能及性能，很好的保护用户的投资。

VSM配置

VSM配置

VSM 模式：无

VSM 状态：☐ 启用

VSM ID：

0

上行级联口②：[去配置](#)

下行级联口②：[去配置](#)

本框优先转发：☐ 启用

分裂监测：☐ 启用

图 15 VSM 虚拟化配置

√ VSM 具有以下主要特点：

- **简化管理。**开启 VSM 模式后，用户通过任意成员设备的任意端口均可以主（Master）设备页面对 VSM 内所有成员设备进行统一管理，而不用物理连接到每台成员设备上分别对它们进行配置和管理。
- **简化网络结构。**VSM 形成的虚拟设备中运行的各种控制协议也是作为单一设备统一运行的，可大大简化网络结构。
- **高可靠性。**VSM 的高可靠性体现在多个方面，例如：成员设备之间 VSM 物理端口支持聚合功能，VSM 系统和上、下层设备之间的物理连接也支持聚合功能，这样通过多链路备份提高了 VSM 系统的可靠性；VSM 系统由多台成员设备组成，Master 设备负责 VSM 系统的运行、管理和维护，Slave 设备在作为备份的同时也可以处理业务，一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证通过 VSM 系统的业务不中断，从而实现了设备的双机备份。

■ **高性能。**由于 VSM 系统是由两个或多个支持 VSM 特性的单机设备虚拟化而成的，VSM 系统的处理能力和端口数量就是 VSM 内部所有单机设备交换容量和端口数量的总和。因此，VSM 技术能够通过两个或多个单机设备的虚拟化，轻易的将设备的核心交换能力、用户端口的密度扩大数倍，从而大幅度提高了设备的性能。

■ **多种级联方式。**在框式设备中，VSM 支持多种单板作为级联板，满足客户不同的需求，目前支持 4*10GE、8*10GE 等单板级联。

■ **丰富的功能。**所有单台设备所支持的功能都能很好的在 VSM 下得到支持。

3.8.3 N:M 虚拟化技术

迪普科技创新的推出了 N:M 虚拟化技术，首先运用 VSM 虚拟化技术将多台设备虚拟成一台（N-->1），继而将这一台设备运用虚拟防火墙技术将一台 VSM 系统虚拟成多台虚拟防火墙（1-->M），从而实现 N:M 的虚拟化技术。

- 将 N 台框式设备级联，VSM 虚拟成一台设备
- 将级联后的设备虚拟成 M 台逻辑子设备分配给相应管理员独立管理和使用
- 按需扩展处理性能、端口密度、虚拟防火墙数量

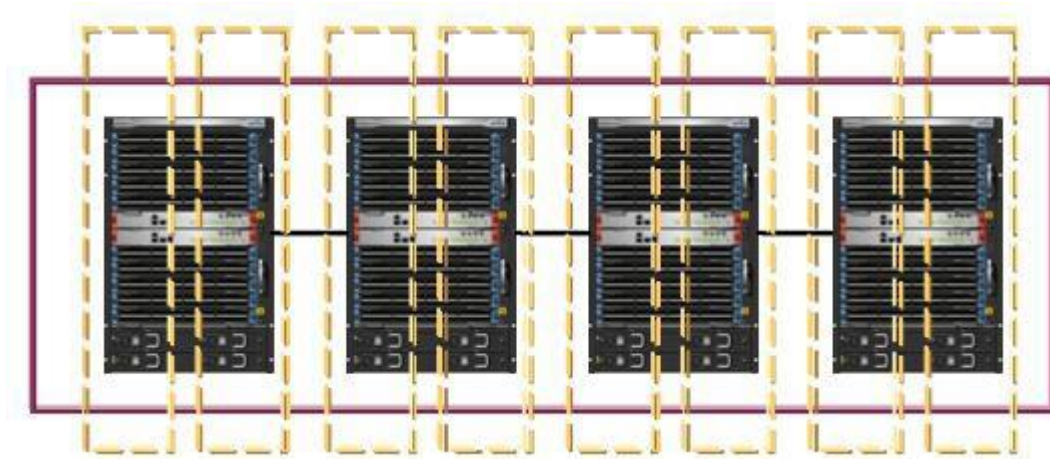


图 16 N:M 虚拟化技术

N:M 虚拟化实现安全云计算：

- 高性能单板处理能力
- 大容量背板交换能力，支持多框级联，通过插板和插框拓展整机处理能力
- 集网络安全、应用交付、业务交换于一体，全方位保障云计算的安全
- 操作系统级虚拟化，从管理、协议、转发、资源等方面全方位虚拟化，将一台设备虚拟成多台设备独立使用，使得安全成为云计算的一种服务

3.8.4 防火墙NFV技术

迪普科技防火墙支持NFV技术，支持按需分配服务器资源，同时支持一虚多虚拟化，同一个虚拟机可再次虚拟化为多个虚墙，为用户提供多租户安全防护，该产品部署简单、灵活，具备以下特点：

- 可提供ISO/QCOW2等主流镜像格式，创建虚拟机灵活度高
- 可运行于X86、ARM、ARM64等硬件平台，同时兼容适配多款国产化硬件平台
- 可运行于KVM、VMware等主流虚拟化平台
- 支持OpenStack纳管对接，可提供完整的OpenStack插件进行纳管对接
- 支持业界主流云平台纳管，为公有云、私有云租户提供防护能力

3.10 支持完善的策略管理功能

- 支持安全策略自动生成，防火墙根据策略分析用户业务，自动生成安全策略，为新建数据中心策略配置运维提供支撑
- 支持安全策略冗余分析，防火墙可以对已有策略进行分析，输出冗余关系，为策略瘦身提供数据支撑
- 支持垃圾策略分析，防火墙可以对历史策略进行筛选，输出垃圾策略清单，为用户策略清理提供支撑

