紫光集团 核心企业 | H3C 数字化解决方案领导者

新华三分销安全
产品手册

新华三集团

新华三商业

新华三集团

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

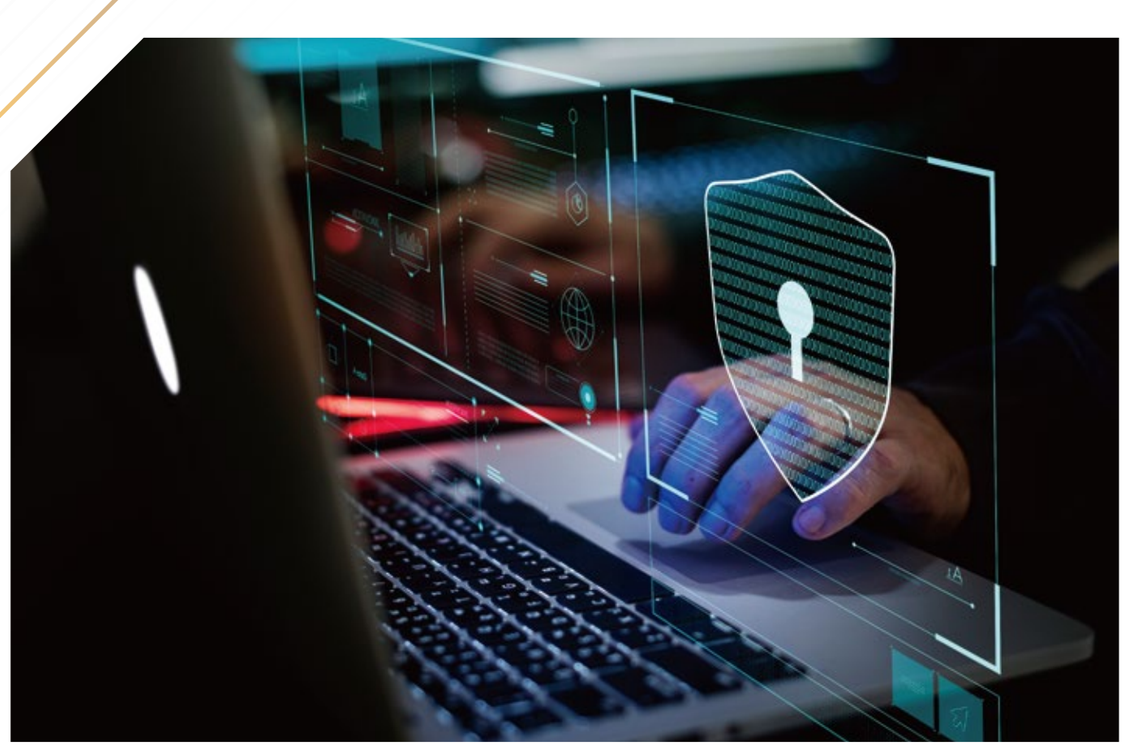
www.h3c.com
客服热线：400-810-0504

CN-202030-20210519-BR-HZ-V3.0

CONTENTS

目录

01 新华三分销安全概述



新华三分销安全产品概述

全产业数字化转型时代，新华三分销安全致力于为数字化的网络安全保驾护航。2017年到2020年，分销安全产品爆发式增长，团队不断壮大，覆盖防火墙、应用控制网关ACG、IPS、负载均衡4类55+款型产品。产品可提供通用等保二级、等保三级、VPN远程办公、云端运维等全场景解决方案，为中小微企业的网络安全保驾护航。

新华三安全领航者

IDC 2020Q1-Q4中国安全市场份额

UTM防火墙 20.1%	NO.3	负载均衡 13.25%	NO.3
入侵防御 13.31%	NO.3	行为管理 5.82%	NO.4

2020Q1-Q4,中国安全硬件市场份额第二
2017年-2020年连续四年入围Gartner魔力象限!

中国网络安全资质和能力领先

- CNNVD一级技术支撑单位
- CNVD技术组成员
- 信息安全风险评估服务 资质一级
- 信息安全应急处理服务资质一级
- 信息安全服务资质证书（安全工程类一级）
- 信息安全等级保护安全建设服务能力评估合格证书
- 商用密码产品销售许可证
- 商用密码产品生产定点单位证书
- 中国国家信息安全产品认证证书
- 公安部计算机信息系统安全 销售许可证
- 信息技术产品安全测评证书EAL4+
- CNCERT网络安全应急服务支撑单位
- IPv6-Ready证书
- IPv6第二阶段增强型认
- 工信部电信设备进网许可证
- 商用密码产品型号证书

专业安全能力 齐全安全资质

02

新华三分销安全产品介绍

H3C SecPath G3系列防火墙

产品定位

◆H3C SecPath G3系列防火墙,是新华三分销安全海量产品的经典畅销款型。

◆产品型号包含F100-X-G3和F1000-X-G3等9款型号。

◆产品性能覆盖由低到高，可广泛完整覆盖中小企业市场。

F100-X-G3系列

产品型号	产品图片	产品描述	带机量（人数）
F100-C-G3		8千兆电口+2COMBO（含1 MGMT）+2BYPASS 单电源，1硬盘扩展插槽,自带100条SSL VPN	400
F100-S-G3		8千兆电口+2COMBO（含1 MGMT）+2BYPASS 1硬盘扩展插槽,,单电源,自带100条SSL VPN	600
F100-M-G3		8千兆电口+2COMBO（含1 MGMT）+2BYPASS 1硬盘扩展插槽,,单电源,自带100条SSL VPN	800
F100-A-G3		16千兆电口（含1MGMT）+8千兆光口,1接口扩展插槽 1硬盘扩展插槽,自带双电源,自带100条SSL VPN	1200
F100-E-G3		16千兆电口（含1MGMT）+8千兆光口, 2接口扩展插槽 1硬盘扩展插槽,自带双电源,自带100条SSL VPN	1500

F100-X-G3系列选配板卡

产品型号	产品描述
NSQM1GT4PFC	4端口千兆电接口卡，自带PFC功能
NSQM1GP4FBA	4端口千兆光接口卡
NS-NIM-TG4A3	4端口万兆接口卡

F1000-X-G3系列

产品型号	产品图片	产品描述	带机量（人数）
F1000-C-G3		2管理口+14千兆电口+12千兆光口+4万兆光口 2接口扩展插槽, 1硬盘扩展插槽,选配双电源 自带100条SSL VPN	2000
F1000-S-G3		2管理口+14千兆电口+12千兆光口+4万兆光口 4接口扩展插槽, 1硬盘扩展插槽,选配双电源 自带100条SSL VPN	3000
F1000-A-G3		2管理口+14千电口+8千兆光口+8万兆光口 4接口扩展插槽, 1硬盘扩展插槽,选配双电源 自带100条SSL VPN	4000
F1000-E-G3		2管理口+14电口+8千兆光口+8万兆光口 4接口扩展插槽, 1硬盘扩展插槽,选配双电源 自带100条SSL VPN	5000

F1000-X-G3系列选配板卡

产品型号	插槽位置	产品描述
NS-NIM-TG6A	Slot1&3：高速插槽	6端口万兆SFP+接口卡
NSQM1GT4PFC	Slot2&4：低速槽	4端口千兆电接口卡，自带PFC功能
NSQM1GP4FBA	Slot2&4：低速槽	4端口千兆光接口卡
NSQM1TG4FBA	Slot2&4：低速槽	4端口万兆接口卡

选配硬盘类型

产品型号	产品描述
NS-HDD-500G-SATA-SFF	H3C SecPath系列,500GB 2.5inch SATA HDD 硬盘模块
NS-SSD-480G-SATA-SFF	H3C SecPath系列,480GB 2.5inch SATA SSD 硬盘模块
NS-HDD-1T-SATA-SFF	H3C SecPath系列,1TB 2.5inch SATA HDD 硬盘模块

F1000-X-G3必配电源

产品型号	产品描述
PSR250-12A1	250W交流电源模块
PSR450-12D	450W 直流电源模块
PSR450-12AHD	450W 高压直流电源模块

产品特点

强大的安全防护功能

◆支持丰富的攻击防范功能。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、地址扫描、端口扫描等攻击防范，还包括针对SYN Flood、UPD Flood、ICMP Flood、DNS Flood等常见DDoS攻击的检测防御。

◆最新支持SOP 1:N完全虚拟化。划分多个逻辑的虚拟防火墙，可基于虚拟系统进行吞吐、并发、新建、策略等性能分配。

◆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。

业界领先的IPv6

◆全面的应用层流量识别与管理。

◆入侵防护:基于精确状态的全面检测引擎,超过7800种攻击特征库，具有极高的入侵检测精度。

◆实时病毒防护: 高性能病毒引擎，可防护500万种以上的病毒和木马，病毒特征库每日更新。

◆海量URL过滤: 支持本地+云端方式，139个分类库，超2000万条URL规则。

◆数据防泄漏（DLP）:支持邮件过滤，提供SMTP邮件地址、标题、附件和内容过滤；支持网页过滤，提供HTTP URL和内容过滤；支持网络传输协议的文件过滤。

灵活可扩展的一体化DPI深度安全

◆支持IPv6状态防火墙，真正意义上实现IPv6条件下的防火墙功能，同时完成IPv6的攻击防范。

H3C SecPath HI系列防火墙

产品定位

◆H3C SecPath F100-S-HI、F100-C-HI、F100-A-HI、F1000-C-HI防火墙是新华三面向中小企业的百兆、千兆防火墙VPN集成网关产品，硬件上基于多核处理器架构，为1U的独立盒式防火墙。

产品型号	产品图片	产品描述	带机量（人数）
F100-C-HI		8*GE+2Combo+2Bypass 2个USB口，无扩展插槽；单电源；自带100条SSL VPN 1硬盘扩展（480G SSD/500G SATA）	600
F100-S-HI		8*GE+2Combo+2Bypass 2个USB口，无扩展插槽；单电源 1硬盘扩展（480G SSD/500G SATA）	800
F100-A-HI		16GE+8SFP，2个USB口，1个扩展插槽 双电源，一个硬盘扩展 （480G SSD/500G SATA）	1500
F1000-C-HI		16GE+8SFP，2个USB口，2个扩展插槽 双电源，一个硬盘扩展 （480G SSD/500G SATA /1T SATA）	4000

产品特点

硬件架构

◆19寸机架式设计
◆丰富端口类型
◆支持断电Bypass

软件性能

◆覆盖1G~5G场景
◆自带100条SSL VPN
◆全面的威胁,病毒特征库

H3C SecPath 桌面防火墙

产品定位

◆H3C SecPath 桌面列防火墙,是面向分销市场的百兆防火墙VPN集成网关产品，硬件上基于多核处理器架构，采用13寸机箱。-W款设备均支持WLAN功能，F100-C-A6-WL还内置4G Modem，可以通过4G接入互联网。
◆可广泛覆盖区县政府，中小学，中小企业分支出口， 保障网络安全。

产品型号	产品图片	产品描述	带机量
F100-C-A3		8GE，13 寸可上机架 外置4G USB，自带15 个SSLVPN	70-100
F100-C-A3-W		8GE，13 寸可上机架，外置4G USB 自带15 个SSLVPN	70-100
F100-C-A5		8GE，13 寸， WIFI 双频 自带100 个SSLVPN	100-120
F100-C-A5-W		8GE，13 寸，WIFI 双频，自带100 个SSLVPN	100-120
F100-C-A6		8GE，13 寸，内置4G 模块，支持移动/ 电信/ 联通 自带100 个SSLVPN	120-150
F100-C-A6-WL		8GE，13 寸，WIFI 双频，内置4G 模块 支持移动/ 电信/ 联通，自带100 个SSLVPN	120-150

产品特点

硬件架构

◆13寸桌面防火墙
◆出厂配挂耳可上机架

简单易用

◆U盘零配置开局
◆IMC平台统一管理，统一运维
◆快速向导，秒级上线
◆SSM-G2安全平台统一管理运维

功能丰富

◆VPN，IPS，AV
◆2.4G和5G双频WI-FI
◆外置4G卡插槽

H3C SecPath 云防火墙系列防火墙

产品定位

◆H3C SecPath F1000-C81X0系列防火墙是新华三伴随Web2.0时代的到来并结合当前安全与网络深入融合的技术趋势，针对中小型企业、园区网互联网出口以及广域网分支市场推出的下一代高性能云防火墙产品。

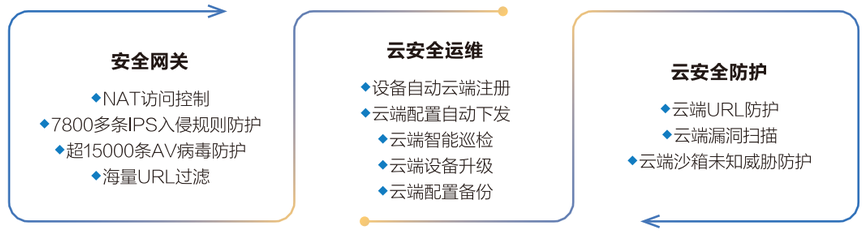
◆F1000-C81X0系列云防火墙旨在通过云管理平台提供的运维管理和安全服务，解决客户安全设备部署、运维困难、安全服务等问题，帮助用户快速开局，云端简化运维，云端实时安全守护。

产品型号	产品图片	产品描述	带机量（人数）
F1000-C8102		8GE+2USB，桌面形态,单电源，13寸 2USB+1硬盘扩展；可上机架	100
F1000-C8110		8GE+2USB，桌面形态,单电源，13寸 2USB+1硬盘扩展；可上机架	200
F1000-C8120		8GE+2BYPASS+2Combo 2USB 单电源，19寸	500
F1000-C8130		8GE+2BYPASS+2Combo 2USB 单电源，19寸	1000
F1000-C8150		8GE+2BYPASS+2Combo 2USB 自带双电源，19寸	2000
F1000-C8160		16GE+8SFP, 2扩展板卡, 1硬盘扩展 自带双电源，19寸	3000
F1000-C8170		16GE+8SFP+2USB, 2扩展板卡, 1硬盘扩展 自带双电源，19寸	4000
F1000-C8180		16GE+8SFP +2 万兆光+2USB, 2扩展板卡, 2硬盘扩展，选配双电源，19寸	5000

选配电源型号	LSPM2150A：150W交流电源模块	LSPM5150D：150W 资产管理直流电源模块

选配硬盘类型

产品型号	产品描述
NS-HDD-500G-SATA-SFF	H3C SecPath系列，500GB 2.5inch SATA HDD 硬盘模块
NS-SSD-480G-SATA-SFF	H3C SecPath系列，480GB 2.5inch SATA SSD 硬盘模块
NS-HDD-1T-SATA-SFF	H3C SecPath系列，1TB 2.5inch SATA HDD 硬盘模块



云防火墙三大产品特点

产品特点

轻松安全云运维

◆自动云端注册：设备自行向云平台注册，实现设备注册上线、显示在线离线状态、报活等工作。

◆云端设备配置：内置丰富的配置模板，按需一键下发配置，快速上线。

◆设备状态详情：通过云平台可呈现设备详情，包括设备CPU、内存，会话状态等信息。

◆版本管理：设备支持云平台管理对设备的版本文件管理、License管理。可实现云平台日志管理。可接收设备上报的日志，在云端查询设备日志并通过图表呈现日志信息。

◆分级分权限控制：支持云端管理员的创建及权限控制，可分配管理员权限/审计员权限，下级管理员可配置是否允许上级用户代理运维，用户支持自注册管理等功能，并可建立最大4级运营账号管理。

◆云端巡检：云端自主设备巡检，检查CPU、内存利用率，磁盘利用率等，设备异常告警，安全日志，以及详细的设备修改建议。

全面的安全云服务

◆云端漏扫：提供云端自主综合漏洞扫描系统，关注OWASP TOP10的风险评估，丰富的漏扫扫描知识库，完成系统网络安全状况评估体检。包含Web扫描、数据库扫描、系统扫描等全面的漏扫功能，提供详细的修复建议。

◆云端日志审计：云端自主选择对ICT设备和应用系统提供详尽设备日志审计。

◆云端应用监控：依托云的应用监控服务，通过DNS探测、ping、http请求等综合分析应用状况。

H3C SecPath AI系列防火墙

产品定位

◆H3C SecPath F1000-9X0-AI是面向行业市场的高性能多千兆和超万兆防火墙VPN集成网关产品，硬件上基于多核处理器架构，为1U独立盒式防火墙。该系列防火墙产品提供丰富的接口扩展能力。同时作为NGFW产品，丰富的审计功能是必不可少的，所以产品系列可以扩展大容量硬盘，同时增加硬盘后还可以有效支持web缓冲等应用加速功能。

◆在安全功能方面，作为NGFW产品，除支持安全控制、VPN、NAT、DOS/DDOS防御等防火墙安全功能外，还一体化地集成了IPS、AV、应用控制、DLP、URL分类及自定义过滤等深度安全防御的功能，实现了基于用户、应用、时间、地理位置、安全状态等多维度的策略控制功能。

◆产品系列集成了AI计算能力，针对未知威胁和APT攻击提供有力的防护。基于AI技术，简化防火墙产品的运维体验。

产品型号	产品图片	产品描述	带机量（人数）
F1000-905-AI		8千兆电口，内置单电源	200
F1000-910-AI		8千兆电口+2Combo+2Bypass口，内置单电源	500
F1000-920-AI		15千兆电口+8千兆光口+1管理口，内置交流双电源	700
F1000-930-AI		15千兆电口+8千兆光口+4万兆光口+1管理口 内置交流双电源	900
F1000-950-AI		15千兆电口+8千兆光口+4万兆光口+1管理口 内置交流双电源	1200
F1000-960-AI		15千兆电口+8千兆光口+4万兆光口+1管理口 内置交流双电源	2000
F1000-970-AI		15千兆电口+8千兆光口+4万兆光口+1管理口 内置交流双电源	3000
F1000-980-AI		15千兆电口+8千兆光口+6万兆光口+1管理口 选配直流/交流双电源	5000
F1000-990-AI		15千兆电口+8千兆光口+6万兆光口+1管理口 选配直流/交流双电源	6000

可选配电源型号	LSPM2150A：150W交流电源模块	PSR150-D1-B：150W 交流电源模块

产品特点

全面安全防护

◆支持多种NAT访问控制，包括多对一、多对多、一对多、多对一、一对一，源地址目地址同时转换，DNS映射，支持地址转换有效时间设置，支持多种NAT ALG，包括DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP等。

◆H3C SCF虚拟化技术，可将多台设备虚拟化为一台逻辑设备，支持SOP 1:N完全虚拟化。可在H3C SecPath F1000设备上划分多个逻辑的虚拟防火墙，支持CPU、内存、存储等硬件资源划分的完全虚拟化。

◆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。

◆DDOS攻击防范：包括Land、Smurf、Fraggle、Pingof Death、Tear Drop、IP Spoofing、SYN Flood、UPD Flood、ICMP Flood、DNS Flood等DDoS攻击的检测防御。

◆支持丰富VPN功能。包括L2TP、IPSec/IKE、GRE、SSL等，并实现与智能终端对接。

◆链路负载均衡，链路状态检测、链路繁忙保护等技术，有效实现互联网出口的多链路自动均衡和自动切换。

◆数据防泄漏（DLP）：支持邮件过滤，提供SMTP邮件地址、标题、附件和内容过滤；支持网络传输协议的文件过滤。

◆入侵防御（IPS），支持入侵攻击行为的阻断防护，超7800多条IPS入侵规则防护。

◆WEB安全：支持Web攻击识别和防护，如跨站脚本攻击、SQL注入攻击等。

◆应用识别审计：精确检测Thunder/Web Thunder（迅雷/Web迅雷）、BitTorrent、eMule（电骡）/eDonkey（电驴）、微信、微博、QQ、MSN、PPLive等P2P/IM/网络游戏/炒股/网络视频/网络多媒体等应用；支持P2P流量控制功能。

AI智能防护

◆支持https流量的识别与审计。

◆防病毒（AV），高性能病毒引擎，支持流病毒查杀，可防护500万种以上的病毒和木马，病毒特征库每日更新。

◆海量URL分类过滤：支持本地+云端方式，139个分类库，超2000万条URL规则。

◆支持IPv6过渡技术，包括NAT-PT、IPv6 Over IPv4 GRE隧道、手工隧道、6to4隧道、IPv4兼容IPv6自动隧道、ISATAP隧道、NAT444、DS-Lite等。基于IPv6的状态防火墙及攻击防范。

◆支持与态势感知智能联动，设备实时上报威胁日志，当设备遭到攻击，能够智能感知自动下发规则，及时拦截阻断。

◆情报智能IP信誉联动，能够自动过滤具有僵尸主机DDoS攻击、命令注入攻击、木马下载和端口扫描等风险的IP地址集合。

◆支持主动漏洞扫描功能，能够获知特定主机/服务器所开启的UDP/TCP端口号以及基于TCP/UDP的应用服务协议。

◆支持智能安全策略：实现策略冗余检测、策略匹配优化建议、动态检测内网业务动态生成安全策略并推荐。

智能安全防护

◆H3C IMC SSM安全管理中心实现统一管理，统一事件收集、统一分析、联动响应等。

分销安全防火墙授权情况说明

分销安全F100系列产品授权适配情况

产品型号	产品描述
LIS-F100G2-IPS/ACG-1Y	H3C SecPath F100G2 IPS/ACG特征库升级服务授权函,1年
LIS-F100G2-URL-1Y	H3C SecPath F100G2 URL特征库升级服务授权函,1年
LIS-F100-G2-URL-3Y	H3C SecPath F100G2 URL特征库升级服务授权函,3年
LIS-F100G2-IPS-1Y	H3C SecPath F100-G2 IPS 特征库升级服务授权函,1年
LIS-F100G2-AV-1Y	H3C SecPath F100-G2 AV 防病毒安全服务授权函,1年
LIS-F100G2-ACG-1Y	H3C SecPath F100-G2 应用识别特征库升级服务授权函,1年
LIS-F100G2-SSL-30	H3C SecPath F100-G2 SSL VPN 30个用户授权函
LIS-F100G2-SSL-100	H3C SecPath F100-G2 SSL VPN 100个用户授权函
LIS-F100G2-WAF-1Y	H3C SecPath F100-G2 WAF特征库升级授权函,1年
LIS-F100G2-WAF-3Y	H3C SecPath F100-G2 WAF特征库升级授权函,3年
LIS-F100G2-TI-1Y	H3C SecPath F100-G2 安全威胁情报升级服务授权函,1年
LIS-F100G2-TI-3Y	H3C SecPath F100-G2 安全威胁情报升级服务授权函,3年

包含产品型号：F100-X-G3、F100-X-HI、F100-X-G2、F100-C-AX等F100系列防火墙

分销安全防火墙F1000系列产品授权适配情况

产品型号	产品描述
LIS-F1000G2-IPS-1Y	H3C SecPath F1000G2系列防火墙 IPS 特征库升级服务授权函,1年
LIS-F1000G2-IPS-3Y	H3C SecPath F1000G2系列防火墙 IPS 特征库升级服务授权函,3年
LIS-F1000G2-ACG-1Y	H3C SecPath F1000G2系列防火墙ACG 特征库升级服务授权函,1年
LIS-F1000G2-ACG-3Y	H3C SecPath F1000G2系列防火墙 ACG 特征库升级服务授权函,3年
LIS-F1000G2-AV-1Y	H3C SecPath F1000G2系列防火墙 AV 特征库升级服务授权函,1年
LIS-F1000G2-URL-1Y	H3C SecPath F1000G2 URL特征库升级服务授权函,1年
LIS-F1000G2-URL-3Y	H3C SecPath F1000G2 URL特征库升级服务授权函,3年
LIS-F1000-G2-WAF-1Y	H3C SecPath F1000-G2 WAF特征库升级授权函,1年
LIS-F1000-G2-WAF-3Y	H3C SecPath F1000-G2 WAF特征库升级授权函,3年
LIS-F1000-G2-TI-1Y	H3C SecPath F1000-G2 安全威胁情报升级服务授权函,1年
LIS-F1000-G2-TI-3Y	H3C SecPath F1000-G2 安全威胁情报升级服务授权函,3年
LIS-F1000G2-SSL-50	H3C SecPath F1000G2系列防火墙50用户SSL VPN授权函
LIS-F1000G2-SSL-200	H3C SecPath F1000G2系列防火墙200用户SSL VPN授权函

包含产品型号：F1000-X-G3、F1000-X-HI、F1000-X-G2、F1000-C81X0、F1000-9X0-AI等F1000系列防火墙

分销安全防火墙F1000-C8102系列产品授权适配情况

产品型号	产品描述
LIS-F1000-C8102-IPS-1Y	H3C SecPath F1000-C8102 IPS特征库升级授权函,1年
LIS-F1000-C8102-AV-1Y	H3C SecPath F1000-C8102 AV特征库升级授权函,1年
LIS-F1000-C8102-URL-1Y	H3C SecPath F1000-C8102 URL特征库升级授权函,1年
LIS-F1000-C8102-APP-1Y	H3C SecPath F1000-C8102 App特征库升级授权函,1年
LIS-F1000-C8102-IPS/AV/URL/APP1Y	H3C SecPath F1000-C8102 IPS/AV/URL/App特征库升级授权函,1年

云墙产品F1000-C8102独有的授权

H3C SecPath 应用安全控制网关

产品定位

◆H3C SecPath ACG 1000是新华三新一代应用控制网关，分销传统海量应用控制网关，ACG 1000引入了全方位上网行为管理要素，是面向客户业务而量身定制的全业务网关产品。

◆H3C SecPath ACG 1000能对网络中的网络社区、P2P/IM带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别和控制。利用智能流控、智能阻断、智能路由等技术，配合创新的社交网络行为管理功能、清晰易管理日志等功能，提供业界最全面、完善的上网行为管理解决方案。

产品型号	产品图片	端口描述	带机量（人数）
ACG1005-PWR		10GE电口+1SFP(含4POE)，TF卡扩展 选配：LIS-ACG1005-PWR-1Y (一年应用识别&URL特征库升级)	100
ACG1010-X1		10GE电口+1SFP，TF卡扩展 选配：LIS-ACG1010-X1-1Y (一年应用识别&URL特征库升级)	200
ACG1030-X1		10GE电口+4GE Combo，内置1T硬盘 选配：LIS-ACG1030-X1-1Y (一年应用识别&URL特征库升级)	500
ACG1050-X1		10GE电口+4GE Combo(含8POE)，内置1T硬盘 选配：LIS-ACG1050-X1-1Y (一年应用识别&URL特征库升级)	800
ACG1060-X1		12GE电口+12SFP ，内置2T硬盘 选配：LIS-ACG1060-X1-1Y (一年应用识别&URL特征库升级)	1000
ACG1070-X1		12GE电口+12SFP，内置2T硬盘 选配：LIS-ACG1070-X1-1Y (一年应用识别&URL特征库升级)	1200
ACG1000-ME		12GE电口+12SFP，内置2T硬盘 选配：LIS-ACG1000-ME (一年应用识别&URL特征库升级)	3000
ACG1000-AE		12GE电口+12SFP+2SFP+ ，1扩展插槽，内置2T硬盘 选配：LIS-ACG1000-AE (一年应用识别&URL特征库升级)	6000

ACG硬盘容量全新升级

◆2020年11月之前发货的硬盘为产品描述硬盘容量的1/2倍。

授权说明

◆ACG1000设备默认包含一年应用识别&URL特征库升级

新增品类	产品型号	产品描述
IPS&AV授权	LIS-ACG1000-X1-IPS/AV-EXT-1Y	License授权函-H3C SecPath ACG10X0-X1 系列-ACG10X0-IPS/AV 特征库升级服务授权-1年-国内版
无线非经模块	LIS-ACG1000 SDK	License授权函-H3C SecPath ACG1000- NSQM1ACG1KSDK1Y-非经 SDK功能授权-1年-国内版

硬盘说明

◆ACG1005-PWR、ACG1010-X1不内置硬盘，但支持TF卡扩展。

说明：TF卡需自行采购，当前仅支持闪迪品牌，8G~128G容量、TLC芯片、CLASS10类型的TF卡（SANDISK:SDSQUNC-064G-ZN3MN），请注意选择的TF卡型号。

◆ACG1030-X1、ACG1050-X1内置500G硬盘，ACG1070-X1、ACG1000-ME、ACG1000-AE内置1T硬盘。

说明：这些型号内置硬盘，不支持TF卡扩展。

授权说明

新增LIS-ACG1000 SDK无线非经授权模块说明

◆广州、深圳、上海、重庆、河南等网监不能直接ACG进行无线非经对接的区域，特引入任子行非经SDK对接模式。

流程：购买SDK授权导入ACG，ACG自动开启该功能向任子行云平台传数据，入围、网监对接、数据核实等工作均由任子行完成，有非经需求的上述项目一定均上此编码做对接,所有ACG1000产品均对应此编码。

ACG Manager系列日志分析与管理软件

授权品类	产品型号	产品描述
高端授权	LIS-ACG1000 Manager-M/A/E	涉及到ACG1060-X1/1070-X1 1000-ME/1000-AE的设备 都需要同时购买高端授权和数量授权 设备数量上限为3000台
数量授权	LIS-ACG1000 Manager-10	低端设备管理数量大于10台时需要购买 高端设备必须购买 设备数量上限为3000台

选配注意

当低端ACG设备：ACG1005-PWR/1010-X1/1030-X1/1050-X1，管理数量<10台时，日志分析与管理软件可以在网站下载,管理软件不需要授权。

高端设备：ACG1060-X1/1070-X1/1000-ME/1000-AE,若仅购买高端授权（M/E/A）：设备数量上限为0台，不允许纳管任何设备。

高端设备：需要既购买数量授权也购买高端授权：设备数量上限为3000台，低端高端设备均可纳管。

ACG Mannager功能

◆集中管理

统一运维：多台ACG，可纳管所有ACG产品，做产品大屏运维展示。

◆策略集中下发

当多台ACG需要调整策略时，manager上统一配置，集中下发，各个设备的策略及配置即可生成。

◆日志收集备份

网络安全法要求审计类产品存储180天以上，且具有备份。ACG本地硬盘空间有限，可存的日志时长有限，可通过manager扩展存储空间作为合规备份，也可充当外置数据中心。

◆提供业界唯一非经平台

Manager管理平台可将全部ACG非经日志收集上来，集中与当地网监做合规对接。

H3C SecPath 云应用安全控制网关

产品定位

SecPath　ACG1000-C91X0系列是新华三推出的最新一代云应用控制网关。该产品可以路由模式、透明桥接模式、旁路模式以及混合模式部署在网络的关键节点。其融合了应用控制、行为审计、网络优化等全面功能，云运维用于对云环境中应用控制网关等安全设备进行管理、统计、监控、配置、升级、日志查看，从而简化运维过程、提高运维效率、保证运维过程的安全性和可回溯性。

产品型号	产品图片	产品描述	行为审计规模(人数)
ACG1000-C9130		4GE(Combo)+10GE(电)，内置硬盘容量1T， 单电源	700
ACG1000-C9150		12GE（光）+12GE（电），内置硬盘容量2T 自带双电源	1100
ACG1000-C9160		12GE（光）+12GE（电），内置硬盘容量2T 自带双电源	3200
ACG1000-C9170		12GE（光）+12GE（电）+2万兆，内置硬盘容量2T 1扩展板卡插槽，自带双电源	6500

说明：ACG1000设备默认包含一年应用识别&URL特征库升级

ACG硬盘容量全新升级

◆2020年11月之前发货的硬盘为产品描述硬盘容量的1/2倍。

选配注意

ACG1000-C9130 TF卡需自行采购，当前仅支持闪迪品牌，8G~128G容量、TLC芯片、CLASS10类型的TF卡（SANDISK:SDSQUNC-064G-ZN3MN），请注意选择的TF卡型号。

云ACG产品授权适配情况

产品型号	产品描述
ACG1000-C9130	LIS-ACG1000-C9130-1Y（一年应用识别&URL特征库升级）
ACG1000-C9150	LIS-ACG1000-C9150-1Y（一年应用识别&URL特征库升级）
ACG1000-C9160	LIS-ACG1000-C9160-1Y（一年应用识别&URL特征库升级）
ACG1000-C9170	LIS-ACG1000-C9170-1Y（一年应用识别&URL特征库升级）
LIS-ACG1000-C-IPS/AV-1Y	ACG1000-C9100-IPS/AV特征库升级服务授权-1年-国内版
LIS-ACG1000 SDK	License授权函-H3C SecPath ACG1000-NSQM1ACG1KSDK1Y-非经SDK功能授权-1年-国内版

说明：新增LIS-ACG1000 SDK无线非经授权模块说明

选配注意

广州、深圳、上海、重庆、河南等网监不能直接ACG进行无线非经对接的区域，特引入任子行非经SDK对接模式。

流程：购买SDK授权导入ACG，ACG自动开启该功能向任子行云平台传数据，入围、网监对接、数据核实等工作均由任子行完成，有非经需求的上述项目一定均上此编码做对接,所有ACG1000产品均对应此编码。

云ACG云端安全产品特点

轻松安全云运维

自动云端注册：设备自行向云平台注册，实现设备注册上线、显示在线离线状态、报活等工作。

云端设备配置：内置丰富的配置模板，按需一键下发配置，快速上线。

设备状态详情：通过云平台可呈现设备详情，包括设备CPU、内存，会话状态等信息。

版本管理：设备支持云平台管理对设备的版本文件管理、License管理。可实现云平台日志管理。可接收设备上报的日志，在云端查询设备日志并通过图表呈现日志信息。

分级分权限控制：支持云端管理员的创建及权限控制，可分配管理员权限/审计员权限，下级管理员可配置是否允许上级用户代理运维，用户支持自注册管理等功能，并可建立最大4级运营账号管理。

云端巡检：云端自主设备巡检，检查CPU、内存利用率，磁盘利用率等，设备异常告警，安全日志，以及详细的设备修改建议。

全面的安全云服务

◆云端漏扫，提供云端自主综合漏洞扫描系统，关注OWASP TOP10的风险评估，丰富的漏扫扫描知识库，完成系统网络安全状况评估体检。包含Web扫描、数据库扫描、系统扫描等全面的漏扫功能，提供详细的修复建议。

◆云端日志审计云端自主选择对ICT设备和应用系统提供详尽设备日志审计。

◆云端应用监控：依托云的应用监控服务，通过DNS探测、ping、http请求等综合分析应用状况。

ACG1000产品特点

场景丰富，功能全面

◆领先的多核架构及分布式搜索检测引擎，配合高性能的处理器，多业务并行处理，确保ACG1000在各种大流量、复杂应用的环境下，仍能具备快速高效的业务处理和防护能力。

ACG1000产品集应用控制、行为审计、负载均衡、应用识别、IPSEC VPN/SSL VPN、业务可视、安全认证等功能于一体，为用户提供了一个灵活、高效、全面的网络解决方案。

带宽流量管控

4级流控架构：支持基于用户/组、应用/组、服务、源地址等七元组的方式实现带宽管理细化，满足用户各种带宽管理的需求。

弹性带宽管理：可以使空闲通道不占用大量带宽，减少带宽的浪费，减少因空闲通道占用带宽，流量达到极限出现丢包现象。

流量和在线时长限额：通过预设用户的流量额度或者在线时长的阀值，对应参数超过设置阀值，设备立即对该用户进行惩罚，惩罚方式可选禁止上网或流量限速。

流控策略白名单：重要来宾和企业重要人员可不受流控策略的限制。

精细化应用管控

ACG1000产品采用DPI/DFI融合识别技术，通过对用户流量进行全面的分析，能够深入识别应用的内置动作，系统内置4500+应用，可以基于应用完成细粒度的应用控制。

◆可以对IM聊天、搜索引擎、论坛社区、邮件收发、文件传输、娱乐股票等模块的应用行为、内容、状态等进行细粒度审计，支持QQ和微信聊天内容审计、传输文件还原、文件大小设置。通过应用精细化管理让网络更有序。

全方位的安全防护

入侵防御：超过4000种预定义攻击特征的入侵防御功能。

病毒防护：超300万海量病毒特征，独特实时病毒拦截技术以及高效引擎的病毒防护功能。

WAF级安全防护：有效的防御和预警Web服务器的攻击，包括网页防爬虫、网页防篡改、HTTPS防护、DDoS攻击防护、Web攻击过滤、漏洞防护自学习、防盗链、CSRF攻击检测、CC攻击防护、应用隐藏、防篡改等。

高级威胁防御：包括安全漏洞、木马后门、可以行为、CGI访问、CGI攻击、缓存溢出、拒绝服务、蠕虫病毒、网络数据库攻击、间谍软件、安全扫描、网络设备攻击、欺骗劫持。

VPN：支持4G IPsec VPN加密连接进行链路备份，支持IPsecVPN冷备份功能，支持SSL VPN远程办公接入。

用户认证管理

ACG1000产品提供了丰富的用户认证方式以及用户同步方式，支持本地认证、短信认证、微信认证、AD单点登录、APP认证、二维码认证、混合认证、USB-key认证等多种准入认证，以及AD服务器、Radius服务器、Portal服务器等外接外部认证服务，更好的满足企业对于用户管理要求。

灵活部署、快速开局

ACG1000产品支持透明、路由、旁路和混合等部署模式，可灵活的连接和审计用户网络。

◆U盘零配置功能，配置预先写入U盘，设备现场快速开局。

H3C SecPath 入侵防御系统

产品定位

H3C SecPath T1000系列产品是新华三开发的业界领先的IPS产品。H3C SecPath T1000系列IPS产品部署在客户网络的关键路径上，通过对流经该关键路径上的网络数据流进行4到7层的深度分析，能精确、实时地识别并阻断或限制黑客、蠕虫、病毒、木马、DoS/DDoS、扫描、间谍软件、协议异常、网络钓鱼、P2P、IM、网游等网络攻击或网络滥用，同时，H3C SecPath T1000系列产品还具有强大、实用的带宽管理和URL过滤功能。

产品型号	产品图片	产品描述	带机量(人数)
T1020		16GE+8 SFP端口,2个扩展插槽，1硬盘扩展 含1年AV/IPS/ACG 许可 可选配授权： LIS-T1020-IPS/AV/ACG-1Y LIS-T1020-IPS/AV/ACG-3Y	150~200
T1050		16GE+8 SFP端口, 2个扩展插槽，1硬盘扩展 含1年AV/IPS/ACG 许可 LIS-T1050-IPS/AV/ACG-1Y LIS-T1050-IPS/AV/ACG-3Y	300~500
T1060		16GE+8SFP+2万兆光，2个扩展插槽，2硬盘扩展 含1年AV/IPS/ACG 许可 可选配授权： LIS-T1060-80-IPS/AV/ACG-1Y LIS-T1060-80-IPS/AV/ACG-3Y	500~800

选配板卡类型

产品型号	产品描述
NSQM1GT4PFC	4端口千兆电接口卡，自带PFC
NSQM1GP4FBA	4端口千兆光接口卡
NSQM1TG4FBA	4端口万兆接口卡

产品特点

高性能的软硬件处理平台

SecPathT1000系列采用了专用的64位多核高性能处理器和高速存储器，SecPathT1000系列可以提供高性能安全业务处理能力。采用CPU+Switch架构，CPU进行安全业务处理，Switch实现多业务端口的扩展。

全面的网络安全防御能力

综合安全防御：

集成入侵防御与检测、病毒防护、带宽管理和URL过滤等功能，是业界综合防护技术最领先的入侵防御/检测系统。通过深入到7层的分析与检测，对比历史均值基线对当前时刻的流量进行异常判断。

专业安全团队：

H3C专业安全团队密切跟踪全球知名安全组织和厂商发布的安全公告，经过分析、验证所有这些威胁，生成保护操作系统、应用系统以及数据库漏洞的特征库。

特征库丰富：

特征库覆盖全面，包含了主流操作系统、主流网络设备、主流数据库系统、主流应用软件系统的全部漏洞特征，同时也包含了黑客、蠕虫、病毒、木马、DoS/DDoS、扫描、间谍软件、网络钓鱼、P2P、IM、网游等网络攻击或网络滥用特征。

国际认证：

H3C通过了微软的MAPP (Microsoft Active Protections Program)认证，可以提前获得微软的漏洞信息。攻击特征库通过了国际权威组织CVE（Common Vulnerabilities & Exposures，通用漏洞披露）的兼容性认证，在系统漏洞研究和攻击防御方面达到了业界顶尖水平。并关注国内特有的网络安全状况，及时对国内特有的攻击提供防御。

全球安全趋势跟踪：

通过部署于全球的蜜罐系统，实时掌握最新的攻击技术和趋势，以定期（每周）和紧急（当重大安全漏洞被发现）两种方式发布，并自动或手动地分发到IPS设备中，使用户的IPS设备在漏洞被公布的同时立刻具备防御零时差攻击的能力。

H3C SecPath 负载均衡

产品概述

◆H3C SecPathL100-C和L1000-C负载均衡是新华三面向中小企业和园区网开发的、业界领先的应用交付产品。

◆产品部署在网络的汇聚层，基于特定的负载均衡算法将客户端对应用服务的访问请求合理地分发到各台服务器上，以保证访问的响应速度和业务连续性。

◆H3C负载均衡产品开创性地实现了应用优化、安全与网络的深度融合，具有强大的路由、交换、负载均衡、2-7层安全等功能。

◆负载均衡产品具有高度的弹性伸缩功能，用户可以根据自己的需要灵活选择功能模块，可适应各种复杂的组网环境。

产品型号	产品图片	产品描述	性能
L100-C		8*GE电口+2*COMBO+2*BYPASS 单电源、支持500G硬盘扩展	L4吞吐量：1G L7吞吐量：500M
L1000-C		16*GE电口+4*SFP光口，2扩展槽 单电源、支持500G硬盘扩展 选配：NSQM1GT4PFC模块 ，PFC模块 4*GE 接口.支持接口bypass	L4吞吐量：2G L7吞吐量：1G

说明：当做应用交付功能时，参考7层吞吐。

产品特点

强大的硬件平台：采用了专用的64位多核高性能处理器和高速存储器，可以提供千兆应用交付处理性能，提供4~7层服务器负载均衡。

高效的健康检测算法：支持丰富的健康检测算法，可从网络层、应用层全方位的探测、检查服务器及应用的运行状态。在进行健康检测时，采用新华三专利NQA（Network Quality Analyzer，网络质量分析）技术，确保健康检测占用最小的系统资源开销，从而保证应用交付业务的性能。

链路负载均衡：支持出站、入站链路负载均衡，结合内置的全球ISP IP地址库进行出、入站流量的智能调度，实现基于不同运营商、链路健康度、链路带宽大小等多要素的链路负载均衡。最终达成内、外网访问用户整体访问体验的提升以及多链路带宽资源的互为备份与合理利用。

服务器负载均衡：支持丰富的负载均衡调度算法，可根据具体的应用场景，采用不同的算法。支持的算法包括：轮询、加权轮询、最小连接、加权最小连接、随机、源地址HASH、目的地址HASH、源地址端口HASH等算法。以上负载均衡算法适用于4~7层服务器负载均衡，同时，对于7层服务器负载均衡还支持基于应用特征的分发，例如基于HTTP头域、内容等。

4~7层服务器负载均衡：

4层服务器负载均衡：基于TCP、UDP、IP的各种业务应用，依据报文的L4层特征（IP、端口）进行负载均衡。7层服务器负载均衡：基于L7内容的负载均衡，通过对报文承载的内容进行深度解析，根据应用层的分析结果对报文进行处理或者分发。

SSL卸载和加速：

H3C SecPathL1000-C系列支持SSL卸载功能，将访问内网服务器中的SSL加解密过程由应用交付设备承担，H3C SecPath L1000-C系列与服务器之间可采用非加密或者弱加密的SSL进行通讯，极大的减小了服务器端对SSL处理的压力，从而将服务器的CPU处理能力释放出来。

连接复用：

H3C SecPath L1000-C系列支持TCP的连接复用功能，使用连接池技术，可以将前端大量的客户的HTTP请求复用到后端与服务器建立的少量的TCP长连接上，大大减小服务器的性能负载，减小与服务器之间新建TCP连接所带来的延时，并最大限度减少后端服务器的并发连接数，降低服务器的资源占用。

应用优化：

采用了全代理的模式，全面接管客户端和服务端的应用流量，支持任何层次的协议字段的解析和优化。支持IP/TCP/HTTP等多个参数模板设置，通过对应用参数模板的设置，可以优化应用交付的功能，提升应用交付的性能。

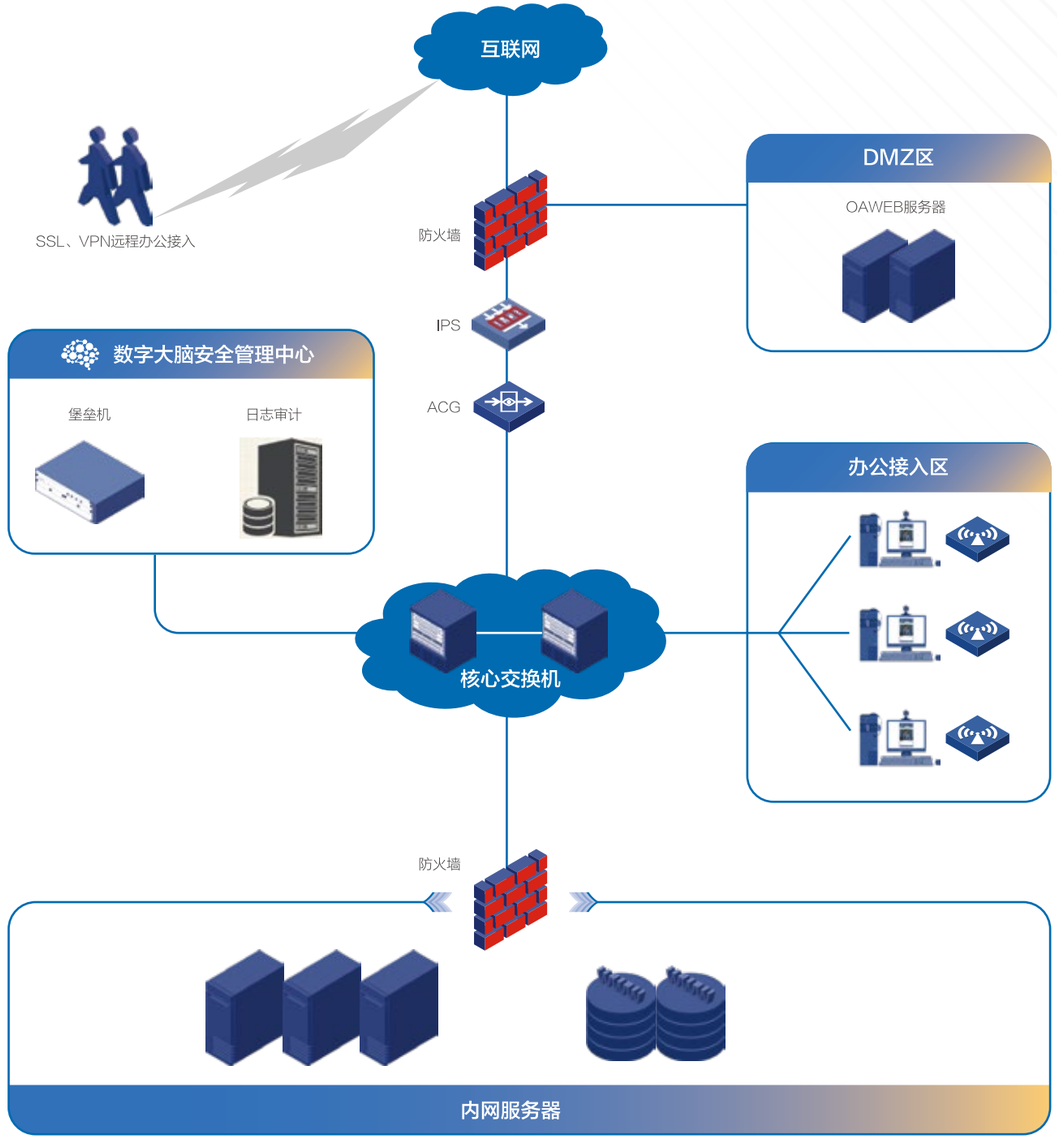
全面的安全防护：

具备全面的安全防护能力，支持对各种DoS/DDoS攻击、ARP欺骗攻击、超大ICMP报文攻击、地址/端口扫描等各种攻击的防范，是业界安全功能极为强大的负载均衡产品。

02

新华三分销安全解决方案

通用等保二级解决方案



设计理念

一个中心，三重防护。

一个数字大脑中心

◆安全管理中心是刚需，符合“系统管理、审计管理、安全管理”集中管控要点。

业务系统重点防护

◆重要业务系统，重点办公区域重点防护，重要Web网站做边界安全防护。

边界防护

◆防火墙：防火墙做非法访问控制，IPS防止入侵攻击和病毒攻击，ACG做上网行为规范，以及无线场所非经对接，满足<公安部81号令>要求。

通信安全

◆边界通信传输通过IPS和AV防病毒保障网络传输安全。

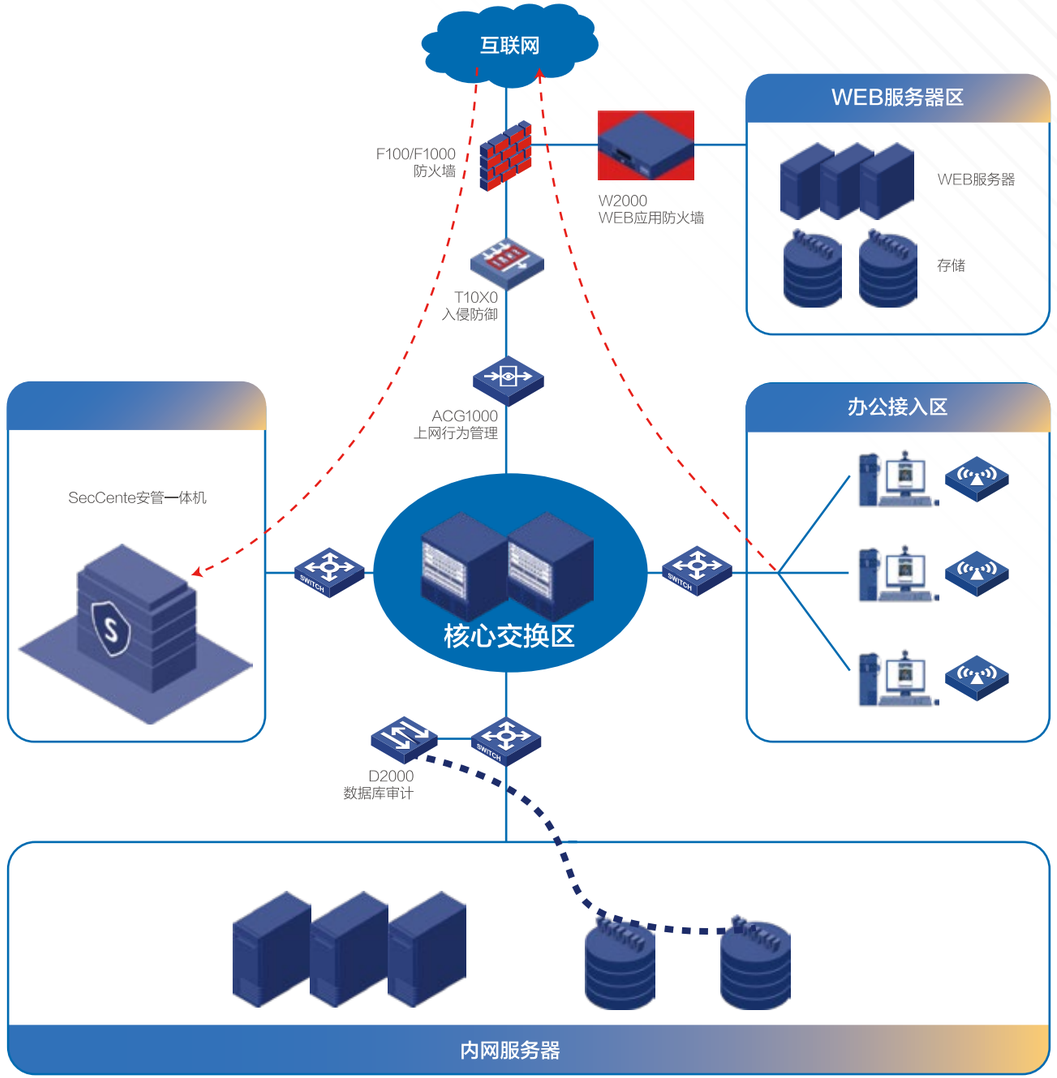
◆远程办公接入，支持国密SM1/SM2/SM3/SM4。

安全管理中心

◆日志审计:推荐款型CSAP-SA-AK640，对全网设备做日志审计留存，同时满足等保的审计要求和国家<<网络安全法>>的180天日志留存需求。

堡垒机:推荐款型A2000-AK610,统一运维管理，等保合规利器，规范用户/运维人员/三方人员做所有网络设备/服务器的业务访问权限和操作审计。

通用等保三级解决方案



设计理念

一个中心，三重防护。

边界安全

◆F100/F1000防火墙，入侵防御做边界权限控制、DDOS、入侵防护、病毒防护。通过U盘零配置和TR069协议设备快速开局。

上网行为安全

◆行为严格管控，上网权限分级分权限，严防数据外泄，高效办公，用户行为画像分析。

安全管理中心

◆包含漏洞扫描，数据库审计，日志审计，运维审计，资产监控等功能，应用配置一键下发，安全事件大屏呈现，脆弱性态势大屏呈现，带外管理，部署简单，实施风险小。

通信安全

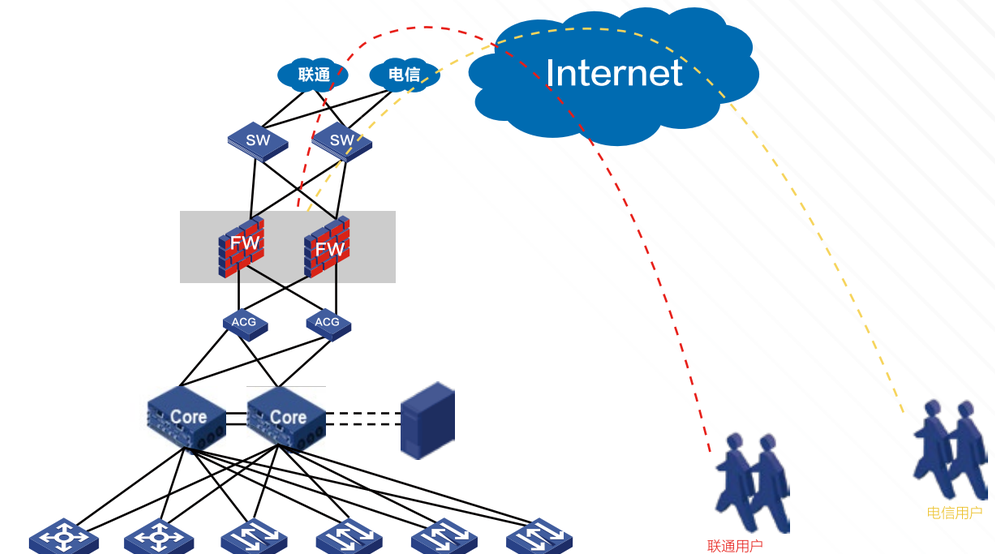
◆边界通信传输通过IPS和AV防病毒保障网络传输安全。

◆远程办公接入，支持国密SM1/SM2/SM3/SM4。

方案优势

◆一体化的管理，零配置的上线技术，后期运维统一化的管理，满足等保2.0等保三级要求。

远程办公解决方案



丰富的功能及强适应性

VPN客户端iNode具有丰富的功能及极强OS适应性，支持windows、Linux、MAC OS、Android、IOS系统。

高可靠性

◆NGFW防火墙采用双机SCF部署，保证VPN网关的可靠性，并且双机虚拟成一台设备，易于管理；IMC EIA可支持采用双机部署方式进一步提高可靠性。

高开放性

◆SSL VPN可支持LDAP/AD认证方式，且可支持CA证书认证。

可支持智能选路

◆可以根据接入用户所属的运营商线路，接入链路的健康状况、拥塞状态智能地选择最佳的支持接入线路，从而达到到最优的访问体验。

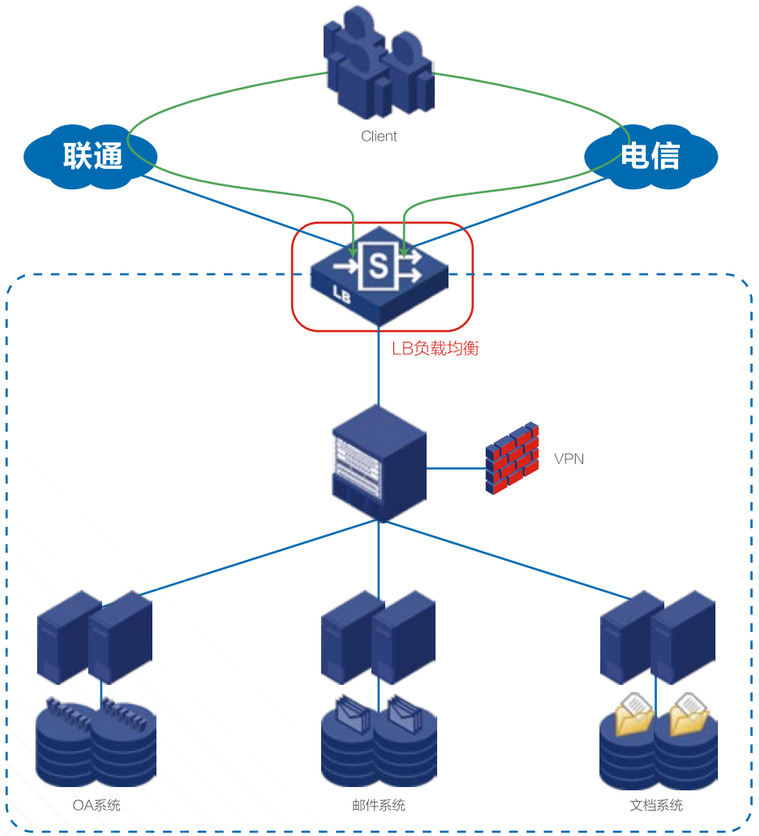
WEB压缩技术

◆H3C SSL VPN支持通过压缩技术减少网络中传递的载荷，改善用户的访问体验。

特征绑定

◆一体化的管理，零配置的上线技术，后期运维统一化的管理，满足等保2.0等保三级要求。

负载均衡智能DNS解决方案



解决方案说明

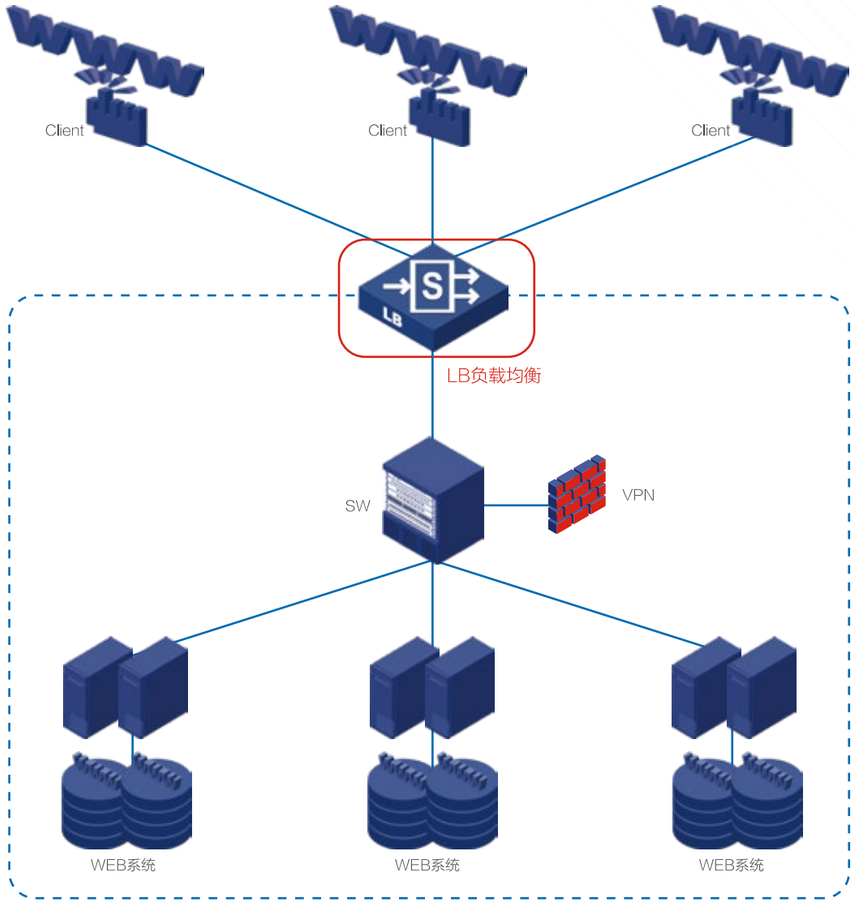
通过智能DNS，做到DNS的有序应答：

1、避免跨运营商访问，始终应答客户端最快链路。

2、拥塞控制，DNS应答过程中会引入剩余带宽作为参考指标。

3、健康度监控，链路发生故障时，实现DNS应答的快速切换。

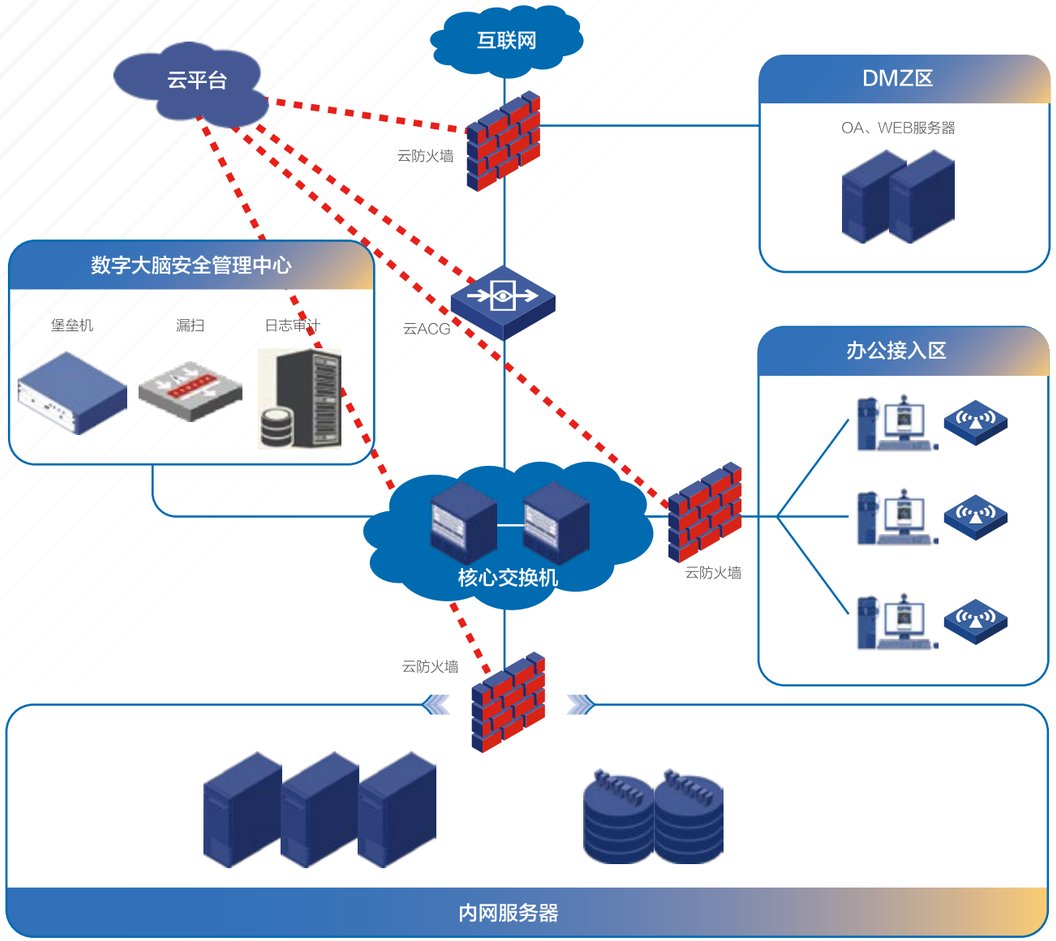
负载均衡应用加速解决方案



解决方案说明

- DRX方案，动态弹性扩展服务器计算容量。
- HTTP在线压缩，节约带宽（压缩比10-60）。
- TCP连接复用，大幅度节约socket（复用比5-18）。
- HTTP高速缓存，节约服务器IO。
- 单边/双边加速，通过优化TCP协议栈以及双向压缩，提升业务在互联网上的传输速度。

云端安全运维解决方案



解决方案说明

◆设备快速上线，V通过U盘零配置上线，大型分支机构项目快速上线。设备自动云端注册，云平台可实现统一配置下发。

◆云端可管理产品，安全云平台可管理云墙、云ACG产品；

◆云端安全运维，云端可实现智能巡检，云端配置备份，云端设备配置调整等。

◆云端安全防护，云端漏扫，云端日志审计、云平台安全报告等云端安全防护功能。

04

新华三分销安全经典案例

某月季大观园

某月季大观园，计划建设以月季展示景观营造为主的集科普、休闲、娱乐为一体的专类园，计划投资17.5亿元，总占地1543.125亩，服务于某2019年世界洲际月季大会。

客户需求

◆客户要求高性价比，易于部署运维。

◆云端协同的网络安全防护，具备入侵防御，病毒防护，云端威胁安全防护。

◆实时保护业务系统(售票系统)数据安全，实时云运维响应。

现状分析

◆现有设备老旧，不能满足业务处理需求。

◆票务系统重要性增强，安全防护能力需升级。

◆业务连续性重要性增强，专业运维人员响应时间不及时。

方案价值

◆云墙支持实时安全事件处置能力。

◆安全策略实时调整。

◆实现7*24小时保障。

◆高效配置，云端智能巡检，降低运维难度。

某连锁超市

某连锁超市有限公司是由国有绝对控股的大型零售连锁企业。
经营门店分布在重庆市多个区县以及四川等地的重点社区和商业中心镇。至今已拥有连锁店140多个。

项目背景

◆位于主城九区渝中、渝北等和区县忠县，璧山等，涉及门店数量62个。

◆超市业务系统现有设备功能单一，无法实时备份。

项目需求

◆62个超市分店都需要安全防护和VPN的接入。

◆安全工程师人员缺乏，需要极简运维。

◆防火墙设备需要能集中管理。

◆超市业务系统部署专线网络。

方案价值

◆云平台统一管理62个超市防火墙设备。

◆云端实时运维应急响应，实时监控、实时告警。

◆专线主链路为安全防护防火墙，备份链路为VPN组网。

◆专线链路与拨号VPN链路智能备份，智能链路切换。

某区县幼儿园

四川省某区县教育科技和体育局幼儿园，此次信息化改造项目涉及到16所幼儿园。

项目背景

◆网管人员匮乏，希望打造一个可以统一运维的安全网络。

◆在开局部署及后期维护方面存在较大难题。

项目需求

◆需要产品具有部署简单，管理方便等特点。

方案价值

◆每所幼儿园出口位置部署H3C F1000系列云防火墙。

◆统一云管：云端统一管理16所幼儿园，零配置上线，云端配置，云端实时响应，智能巡检。

◆全功能防护：具备入侵防御功能，防病毒、DDOS防护等的下一代云防火墙，提供网络边界全面防护，为后续等保建设铺垫基石。

◆云安全防护：具备云端URL库、云端未知威胁分析将弥补本地检测能力有限，提供全方位的云端安全防护功能。

◆强扩展性：可扩展IMC做图像分析设备做准入认证，统一管理整体网络,纳管交换机，PC，防火墙，图像采集设备等。

某市交投

项目背景

◆新建5层办公楼，共计200个办公点。

◆客户需要做办公楼的基础网络系统建设，系统主要为内部工作人员提供Internet的安全连接，承载各项数据信息的传输，保障日常工作需求。

项目需求

◆带宽百兆链路接入终端。网络核心交换与网络接入均为千兆链路。

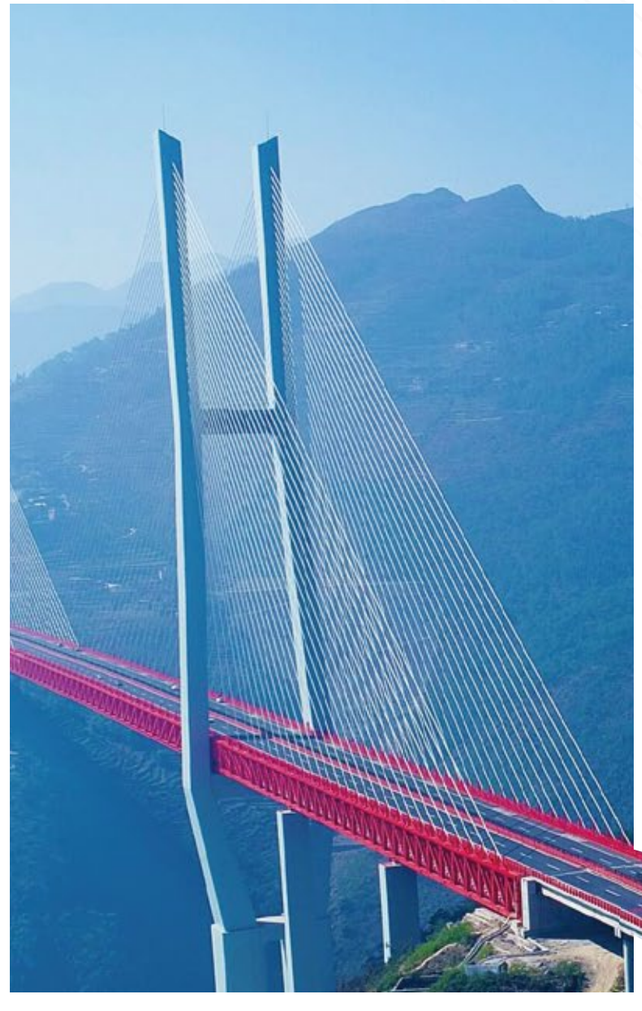
◆对整体网络边界要有一个基础安全防护，　防护DOS攻击，DDOS攻击等四层以下的攻击。

方案价值

◆高性能边界安全网关，限制内外受控资源访问。

◆设备高可用，满足业务扩张扩展需求。

◆安全功能全面，能有效防护边界DDOS，入侵防护，僵尸，勒索 病毒防护。



15000+客户选择我们

电信媒体

CCTV 中国中央电视台

金融

中国工商银行
中国农业银行 AGRICULTURAL BANK OF CHINA
中国银联 China Unionpay
中国银行 BANK OF CHINA
中国邮政 CHINA POST
交通银行 BANK OF COMMUNICATIONS
中信银行 CHINA CITIC BANK
中国银河证券 CHINA GALAXY SECURITIES

政府机关

中华人民共和国人力资源和社会保障部 Ministry of Human Resources and Social Security of the People's Republic of China
中华人民共和国财政部 Ministry of Finance of the People's Republic of China
国家税务总局 State Taxation Administration

互联网

Tencent 腾讯
Baidu 百度 百度一下 你就知道
JD.COM 京东
世纪互联 www.21vianet.com
58同城
滴滴
途牛 tuniu.com
金山 KINGSOFT
搜狐 SOHU.com

能源

SINOPEC
中国石油
国家电网 STATE GRID
中国大唐集团公司 China Datang Corporation
中国南方电网

企业集团

中粮 COFCO
GOME 国美电器
SOHO 3
锦江之星 JINJIANG INN
用友 yonyou
Yum!
中联重科
新兴际华集团

交通运输

中国航信 TravelSky
中国铁路总公司 CHINA RAILWAY
中国南方航空 CHINA SOUTHERN AIRLINES
海南航空 Hainan Airlines
春秋航空
SR

教育

南开大学
吉林大学
华中农业大学
中南财经政法大学 ZHONGNAN UNIVERSITY OF ECONOMICS AND LAW