

# H3C SecPath F1000-GM-AK 系列 VPN 网关

## 产品概述

H3C SecPath 系列 ( F1000-GM-AK370/F1000-GM-AK380 ) VPN 网关是新华三技术有限公司伴随 Web2.0 时代的到来并结合当前安全与网络深度融合的技术趋势，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 VPN 网关产品。

H3C SecPath 系列 ( F1000-GM-AK370/F1000-GM-AK380 ) VPN 网关支持多种 VPN 业务，如 L2TP VPN、GRE VPN 、IPSec VPN 和 SSL VPN 等，与智能终端对接实现移动办公；支持多维一体化安全防护，可从用户、应用、时间、五元组等多个维度，对流量展开 IPS、AV、DLP 等一体化安全访问控制，能够有效的保证网络的安全；提供丰富的路由能力，支持 RIP/OSPF/BGP/路由策略及基于应用与 URL 的策略路由；支持 IPv4/IPv6 双协议栈同时，可实现针对 IPV6 的状态防护和攻击防范。

H3C SecPath 系列 ( F1000-GM-AK370/F1000-GM-AK380 ) VPN 网关采用互为冗余备份的双电源 ( 1 + 1 备份 )，同时支持双机集群化部署的 SCF 技术，充分满足高性能网络的可靠性要求；同时产品在 1U 高的设备上可提供最大 24 个千兆接口、2 个万兆(F1000-GM-AK380)的固定接口。

H3C SecPath F1000-GM-AK370 和 F1000-GM-AK380 均可配置国密算法加密卡，支持 SM1/SM2/SM3/SM4 国密算法。



F1000-GM-AK370



F1000-GM-AK380

## 产品特点

### 高性能的软硬件处理平台

- SecPath F1000-GM-AK 系列采用了专用的多核高性能处理器和高速存储器，可以提供 10G 以下的千兆 VPN 业务处理性能。产品采用 CPU+Switch 架构，CPU 进行安全业务处理，Switch 实现多业务端口的扩展。

### 电信级设备高可靠性

- 采用 H3C 公司拥有自主知识产权的软、硬件平台。产品应用从电信运营商到中小企业用户，经历了多年的市场考验。
- 支持 H3C SCF 虚拟化技术，可将多台设备虚拟化为一台逻辑设备，对外呈现为一个网络节点，资源统一管理，完成业务备份同时提高系统整体性能。

### 强大的 VPN 功能

- CPU 内置高性能加密引擎，确保计算复杂的加解密操作不会对 CPU 处理其他业务造成影响，同时保证了 VPN 的处理性能。
- 支持 GRE VPN、L2TP VPN、IPSec VPN、DVPN、SSL VPN 及多种 VPN 技术的组合应用。
- 支持 IPV6 IPSec VPN、IPV6 GRE VPN。
- 支持多种 VPN 技术的组合使用 IPSec Over GRE，L2TP over IPSec 等。

### 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、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。可在 VPN 网关设备上划分多个逻辑的虚拟 VPN 网关，基于容器化的虚拟化技术使得虚拟系统与实际物理系统特性一致，并且可以基于虚拟系统进行吞吐、并发、新建、策略等性能分配。
- 支持安全区域管理。可基于接口、VLAN 划分安全区域。
- 支持包过滤。通过在安全区域间使用标准或扩展访问控制规则，借助报文中 UDP 或 TCP 端口等信息实现对数据包的过滤。此外，还可以按照时间段进行过滤。
- 支持基于应用、用户的访问控制，将应用与用户作为安全策略的基本元素，并结合深度防御实现下一代的访问控制功能。
- 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网关或者是被丢弃。
- 支持验证、授权和计帐（AAA）服务。包括：基于 RADIUS/HWTACACS+、CHAP、PAP 等的认证。
- 支持静态和动态黑名单。
- 支持 NAT 和 NAT 多实例。
- 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。
- 支持安全日志。

- 支持流量监控统计、管理。

## 灵活可扩展的一体化 DPI 深度安全

- 与基础安全防护高度集成的一体化安全业务处理平台。
- 全面的应用层流量识别与管理：通过 H3C 长期积累的状态机检测、流量交互检测技术，能精确检测 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，通过对流量采用深度检测的方法，即通过将网络报文与 P2P 协议报文特征进行匹配，可以精确的识别 P2P 流量，以达到对 P2P 流量进行管理的目的，同时可提供不同的控制策略，实现灵活的 P2P 流量控制。
- 高精度、高效率的入侵检测引擎。采用 H3C 公司自主知识产权的 FIRST（Full Inspection with Rigorous State Test，基于精确状态的全面检测）引擎。FIRST 引擎集成了多项检测技术，实现了基于精确状态的全面检测，具有极高的入侵检测精度；同时，FIRST 引擎采用了并行检测技术，软、硬件可灵活适配，大大提高了入侵检测的效率。
- 实时的病毒防护：采用流引擎查毒技术，可迅速、准确查杀网络流量中的病毒等恶意代码。
- 全面、及时的安全特征库。通过多年经营与积累，H3C 公司拥有业界资深的攻击特征库团队，同时配备有专业的攻防实验室，紧跟网络安全领域的最新动态，从而保证特征库的及时准确更新。

## 业界领先的 IPv6

- 支持 IPv6 状态检测，真正意义上实现 IPv6 条件下的网关功能，同时完成 IPv6 的攻击防范。
- 支持 IPv4/IPv6 双协议栈，并支持 IPv6 数据报文转发、静态路由、动态路由及组播路由等功能。
- 支持 IPv6 各种过渡技术，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。
- 支持 IPv6 ACL、Radius 等安全技术。

## 专业的智能管理

- 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。
- 支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2。
- 提供图形化界面，简单易用的 Web 管理。
- 可通过命令行界面进行设备管理与 VPN 网关功能配置，满足专业管理和大批量配置需求。
- 通过 H3C IMC SSM 安全管理中心实现统一管理，集安全信息与事件收集、分析、响应等功能为一体，解决了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，采用主动收集、被动接收等方式，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，主要包括基于应用的报表、基于网流的分析报表等。
- 支持以 PDF、HTML、WORD 和 TXT 等多种格式输出。

- 可通过 Web 界面进行报告定制，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。

## 产品规格

| 项目    | F1000-GM-AK370   | F1000-GM-AK380   |
|-------|--|--|
| 接口    | 1个配置口 ( CON )<br>2个外置USB host接口<br>16个千兆以太电口<br>8个千兆以太光口   | 1个配置口 ( CON )<br>2个外置USB host接口<br>16个千兆以太电口<br>8个千兆以太光口<br>2个万兆光口 |
| 扩展槽位  | 2  | 2  |
| 存储介质  | 1个硬盘扩展插槽, 支持扩展SATA硬盘   | 2个硬盘扩展插槽, 支持扩展SATA硬盘   |
| 环境温度  | 工作: 0~45°C<br>非工作: -30~70°C  |  |
| 运行模式  | 路由模式、透明模式、混杂模式   |  |
| AAA服务 | Portal认证、RADIUS认证、HWTACACS认证、PKI/CA ( X.509格式 ) 认证、域认证、CHAP验证、PAP验证  |  |
| VPN   | <p>L2TP VPN</p> <ul style="list-style-type: none"> <li>◆ 支持 LNS</li> <li>◆ 支持 Auto-Initiated LAC</li> <li>◆ L2TP 支持 VRF</li> </ul> <p>GRE VPN</p> <ul style="list-style-type: none"> <li>◆ GRE Over IPV4</li> <li>◆ GRE Over IPV6</li> <li>◆ GRE 支持 VRF</li> </ul> <p>IPSec/IKE</p> <ul style="list-style-type: none"> <li>◆ 安全协议支持 AH/ESP</li> <li>◆ 支持传输和隧道模式</li> <li>◆ ESP 支持 DES、3DES 和 AES 三种加密算法</li> <li>◆ 支持 MD5 及 SHA-1 验证算法</li> <li>◆ 支持通过 manual 或 IKE 方式建立 SA</li> <li>◆ 支持防重放攻击</li> <li>◆ 支持 IPSec 策略模版</li> <li>◆ 支持 IPSec 反向路由注入</li> <li>◆ 支持 IKEV1</li> <li>◆ 支持 IKE 主模式及野蛮模式</li> </ul> |  |

|      |  |
|------|--|
|      | <ul style="list-style-type: none"> <li>◆ 支持通过预共享密钥和证书方式验证 IKE Peer 身份</li> <li>◆ 支持 DPD</li> <li>◆ 支持 IKE Keppalive</li> <li>◆ 支持 NAT 穿越(野蛮模式和主模式)</li> <li>◆ VRF aware : 通过 IKE peer 对端信息确定所属的 VPN</li> <li>◆ 支持 IPSec 双机热备(规划中)</li> <li>◆ 支持 IKEV2</li> </ul>   |
| 防火墙  | <p>基本ACL和高级ACL</p> <p>基于安全区域的访问控制</p> <p>基于时间段的访问控制</p> <p>ASPF状态防火墙</p> <p>DOS/DDOS攻击防范：包括SYN Flood、UDP Flood、ICMP Flood、ACK Flood、RST Flood , DNS Flood、HTTP Flood</p> <p>畸形包攻击如：Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、IP分片报文攻击、分片报文攻击、TCP报文标志位不合法攻击、超大ICMP报文攻击、ICMP重定向或不可达报文</p> <p>扫描窥探攻击防范：端口扫描、地址扫描、IP路由记录选项报文、Tracert报文</p> <p>IP Spoofing攻击防范</p> <p>静态和动态黑名单功能</p> <p>连接数限制</p> <p>支持N:1 SCF集群技术</p> <ul style="list-style-type: none"> <li>◆ 支持多台设备集群</li> <li>◆ 集群设备统一管理</li> <li>◆ 集群设备业务分布式处理</li> </ul> <p>支持1:N虚拟防火墙技术</p> <ul style="list-style-type: none"> <li>◆ 容器化的虚拟化技术，虚拟防火墙特性与物理墙特性一致</li> <li>◆ 虚拟防火墙独立 GUI/CLI 管理</li> <li>◆ 虚拟防火墙独立配置文件</li> <li>◆ 虚拟防火墙独立日志主机及日志审计</li> <li>◆ 虚拟防火墙资源分配：吞吐、并发、新建、策略</li> <li>◆ 虚拟防火墙接口共享</li> <li>◆ N:1:M 虚拟化：先将多台设备集群，然后再进行虚拟防火墙划分</li> </ul> |
| 病毒防护 | <p>基于病毒特征进行检测</p> <p>支持病毒库手动和自动升级</p> <p>报文流处理模式</p> <p>支持 HTTP、FTP、SMTP、POP3 协议</p>   |

|        |   |
|--------|---|
|        | <p>支持的病毒类型：Backdoor、Email-Worm、IM-Worm、P2P-Worm、Trojan、AdWare、Virus 等</p> <p>支持病毒日志和报表</p>  |
| 深度入侵防御 | <p>支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、DoS/DDoS 等常见的攻击防御</p> <p>支持缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御</p> <p>支持攻击特征库的分类（根据攻击类型、目标机系统进行分类）、分级（分高、中、低、提示四级）</p> <p>支持攻击特征库的手动和自动升级（TFTP 和 HTTP）</p> <p>支持对 BT 等 P2P/IM 识别和控制</p>  |
| 网络协议   | <p>ARP</p> <ul style="list-style-type: none"> <li>◆ 静态 ARP</li> <li>◆ 动态 ARP</li> <li>◆ ARP 代理</li> <li>◆ 免费 ARP</li> </ul> <p>DNS</p> <ul style="list-style-type: none"> <li>◆ 本地静态域名</li> <li>◆ DNS Client</li> <li>◆ DNS Proxy</li> <li>◆ DDNS 动态域名服务</li> </ul> <p>DHCP</p> <ul style="list-style-type: none"> <li>◆ DHCP 中继</li> <li>◆ DHCP 服务器</li> <li>◆ DHCP 客户端</li> </ul> <p>NTP</p> <ul style="list-style-type: none"> <li>◆ NTP Client</li> <li>◆ NTP Server</li> </ul> |
| NAT    | <p>静态路由管理</p> <p>策略路由</p> <p>动态路由</p> <ul style="list-style-type: none"> <li>◆ RIP-1/RIP-2</li> <li>◆ OSPF</li> <li>◆ BGP</li> <li>◆ ISIS</li> <li>◆ 路由策略</li> </ul>  |

|      |   |
|------|---|
|      | <p>组播</p> <ul style="list-style-type: none"> <li>◆ IGMP</li> <li>◆ PM-SM</li> <li>◆ PM-DM</li> </ul>  |
| IPv6 | <p>基于IPv6的状态检测及攻击防范</p> <p>IPv6协议：IPv6转发、ICMPv6、PMTU、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay等</p> <p>IPv6路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由、PIM-SM、PIM-DM等</p> <p>IPv6安全：NAT-PT、IPv6 Tunnel、IPv6 Packet Filter、Radius、IPv6域间策略、IPv6连接数限制等</p> |
| 高可靠性 | <p>支持SCF 2:1虚拟化</p> <p>支持双机状态热备（Active/Active和Active/Backup两种工作模式）</p> <p>支持双机配置同步</p> <p>支持IPSec VPN的IKE状态同步</p> <p>支持VRRP</p>   |
| 易维护性 | <p>支持基于命令行的配置管理</p> <p>支持Web方式进行远程配置管理</p> <p>支持安全管理软件进行设备管理及策略统一下发</p> <p>支持标准网管 SNMPv3，并且兼容SNMP v1和v2</p> <p>智能安全策略</p>   |

## 典型组网

## VPN 应用

SecPath F1000系列集成了丰富的VPN功能，包括IPSec VPN、SSL VPN、L2TP VPN等，可以作为中小型企业的出口网关设备提供移动用户的SSL VPN接入，也可以作为广域网组网的分支或二三级中心设备提供site-to-site的IPSec VPN接入。IPSEC业务和SSL VPN业务支持采用国密算法。



图1-1 VPN 应用组网图-远程接入

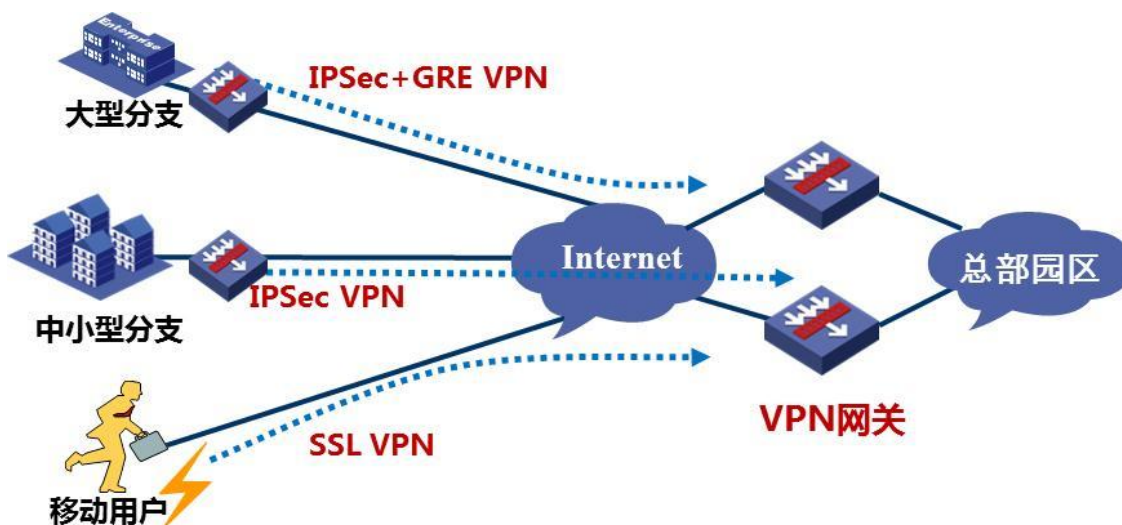
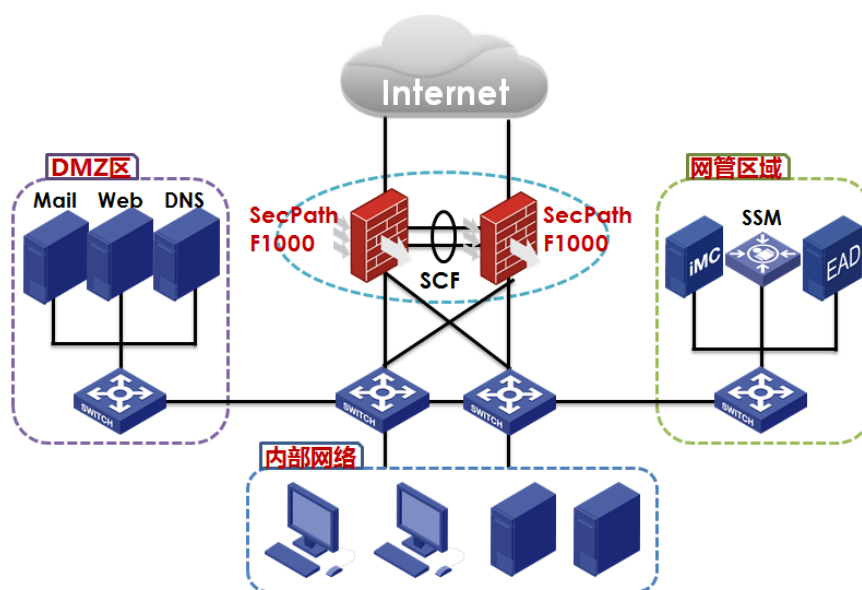


图1-2 VPN 应用组网图-Site-to-Site IPsec VPN



- SCF 2:1 虚拟化技术，高可靠网络设计
- 具有强大的处理能力，支持 GE、10GE 组网
- 丰富路由协议，实现安全与网络融合
- 具有强大的 VPN 加密处理能力
- 全面深度安全防御阻止恶意攻击，同时能够实现邮件、网页、文件过滤

- 丰富路由协议，实现安全与网络融合

## 订购信息

### (1) 主机选购一览表(F1000-GM-AK370/ F1000-GM-AK380)

| 项目  | 数量 | 备注 |
|---|----|----|
| F1000-GM-AK370 Bundle<br>1主机+500G HDD+2内置AC+200 SSL VPN | 1  | 必配 |
| F1000-GM-AK380 Bundle<br>1 主机+500G HDD+1AC++200 SSL VPN | 1  | 必配 |
| 4SFP+ (SMB 专用)  | 1  | 选配 |
| 4PFC (SMB 专用)   | 1  | 选配 |
| 4SFP (SMB 专用)   | 1  | 选配 |
| 2.5 inch 480G SSD 硬盘                                    | 1  | 选配 |
| 500GB SATA HDD 硬盘                                       | 1  | 选配 |
| 1TB SATA HDD硬盘  | 1  | 选配 |

### (2) 电源模块

| 电源模块        | 备注       |
|-------------|----------|
| 150W 交流电源模块 | AK380 选配 |
| 150W 直流电源模块 | AK380 选配 |

⚠ 说明：

“必配”表示所描述项目是设备正常运行的最小配置。

“选配”表示所描述项目是用户根据实际使用需要可选择配置。



**新华三技术有限公司**

杭州基地  
杭州市高新技术产业开发区之江科技  
工业园六和路 310 号  
邮编：310053  
电话：0571-86760000  
传真：0571-86760001  
版本：20120316-V1.0

北京分部  
北京市海淀区知春路 7 号致真大厦 B 座 20 层  
邮编：100052  
电话：010-63108666  
传真：010-63108777

<http://www.h3c.com.cn>

**客户服务热线**

400-810-0504

800-810-0504

Copyright © 2017 新华三技术有限公司 保留一切权利  
免责声明：虽然 H3C 试图在本资料中提供准确的信息，但不保证资料的内容不含有技术性误差或印刷性错误，为此 H3C 对本资料中的不准确不承担任何责任。  
H3C 保留在没有通知或提示的情况下对本资料的内容进行修改的权利。