



H3C SecPath Virtual Firewalls (vFWs)

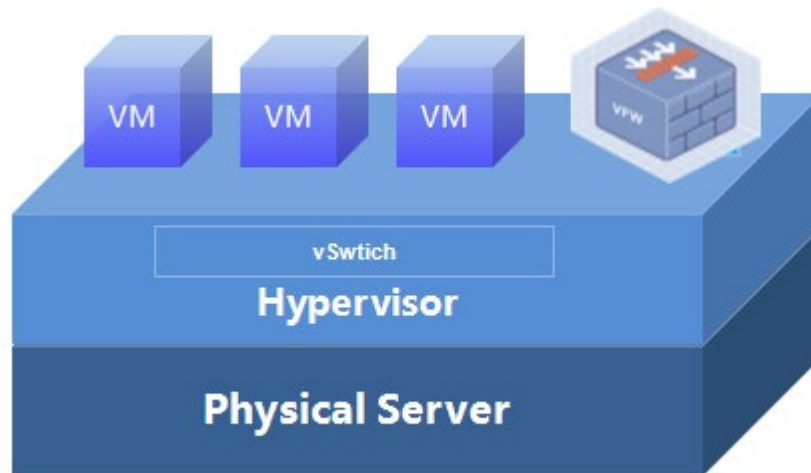
Product overview

H3C SecPath vFWs are a set of powerful software security products that can run on multiple mainstream hypervisors. It runs the cutting-edge H3C Comware 7 operating system, and can monitor and protect the virtual environment and networks from internal and external threats. It delivers comprehensive security protection to virtualized data centers and cloud computing networks, and can help enterprises build complete security solutions for data centers and cloud computing networks.

The vFW offers a comprehensive security protection system, guarantees secure remote access, and delivers rich security features including attack detection and defense, NAT, ALG, ACL, and security zone policies, protecting the network effectively from any possible security threats. With application specific packet filter (ASPF), it monitors the connection process, status, and abnormal commands. It provides a range of intelligent analysis and management methods, supports a variety of logs, offers rich network management and monitoring features, to help network administrators manage network security in high efficiency. It supports setting up many types of VPN connections such as L2TP VPN, GRE VPN, and IPsec VPN connections to ensure secure data transmission over the Internet.

H3C SecPath vFW1000 runs in a VM on a standard server. All its features are license controlled, providing the flexibility for users to select functions, features, and validity periods as needed.

Architecture



Features and highlights

Industry-leading network security platform

Running the industry-leading Comware 7 operating system, the vFW delivers the following benefits:

- Rich network and security functionalities, meeting different network security demands of enterprise branches and public cloud multi-tenant environments.
- Makes full use of computing resources with the control plane and the data plane separated and multi-core data forwarding specifically optimized for the virtual environment.
- Modular architecture and open network platform allow the network to be operated and controlled on demand, making NFV/SDN implementation easier.
- Shares a unified software platform and provides the same features and functionalities and consistent management interface with physical network devices.
- With the service chain technology, it enables dynamic creation and automated deployment of NFV resource pools and allows flexible orchestration and modification of tenant services without affecting the physical topology and other tenants.
- Supporting using NAT64, NAT444, and DS-Lite technologies to enable seamless transition from IPv4 to IPv6.
- Supports license server licensing. Unified license installation, operation, and management on the license server enables automated batch deployment of VNFs. Decoupling licensing from the device and unified licensing allows license pooling and reuse and reduces the licensing cost. This licensing method is highly secure, and can effectively prevent piracy and protect the legitimate rights and interests of users.

Ultra-lightweight deployment

- Suitable for deployment on public clouds, with zero transportation, zero cabling, and accelerated deployment.
- Operable on multiple mainstream supervisors including VMware ESXi, Linux KVM, and H3C CAS, it gives full play to the advantages of virtualization and enables rapid deployment, batch deployment, image backup, rapid recovery, and flexible migration.
- Software images in ISO, OVA, IPE, and QCOW2 formats, adapting to deployment in various environments.
- Supports multiple deployment tools including the VM management platform, network management platform, and local platform, allowing complete flexibility in deployment.
- Allows dynamic creation or deletion of vFW1000s from H3C VNF Manager.

Superb service resiliency

The vFW provides superb service resiliency:

- Operable on multiple mainstream supervisors including VMware ESXi, Linux KVM, and H3C CAS, it can adapt to various deployment environments.
- Allows enterprises to build an enterprise network in a virtualized environment and allocate and manage network resources and services dynamically on demand. For example, the number and type of network interfaces can be flexibly adjusted as needed, eliminating the need to purchase new hardware cards.
- Through dynamic adjustment of virtual resources and licenses, you can upgrade software smoothly and improve device performance on demand as business grows.

Comprehensive security assurance

Powerful security protection features

Packet filtering

Allows you to apply standard or advanced ACLs on incoming and outgoing packets based on information contained in the packets, such as priority, ToS, UDP or TCP port number. You can also configure time ranges during which packet filtering will be performed.

ASPF

Dynamically determines whether to forward or drop a packet by checking its application layer protocol information and state. ASPF supports inspecting FTP, HTTP, SMTP, RTSP, and other TCP/UDP-based application layer protocols.

Attack defense

Detects and prevents various attacks, including Land, Smurf, Fraggle, ping of death, Tear Drop, IP spoofing, IP fragment, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, IP/port scanning, and common DDoS attacks such as SYN flood, UDP flood, DNS flood, and ICMP flood.

VPN

Supports multiple VPN services, including L2TP VPN, IPsec VPN, and GRE VPN, allowing remote access through dial-up, leased line, VLAN, or tunnel, and establishment of various forms of VPNs such as Internet, intranet, or access VPNs as needed. Combined with firewall, AAA, NAT, and various QoS technologies, the vFW ensures secure, reliable private network service over the open Internet.

Security zone

Allows you to configure security zones based on interfaces and VLANs.

Denylist

Supports static denylist and dynamic denylist.

Routing

Supports static routing, policy-based routing, and dynamic routing protocols such as RIP and OSPF.

Complete NAT solution

Provides many-to-one, address pool, ACL control and other address translation methods, supports multiple different address translation services on one interface, and provides FTP, Telnet, and WWW services through the internal server, delivering a complete NAT solution for users.

In addition to general NAT functions, the vFW can also provide NAT ALG for various application protocols, including VoIP and video multimedia applications such as H323, RAS, SIP, SCCP, and RTSP, PPTP VPN applications, and commonly used applications such as FTP, TFTP, DNS, NBT, ICMP, HWCC, DNS, and ILS.

Advanced security management

The vFW provides various types of logs including real-time attack logs, denylist logs, session logs, and NAT logs, which provide a sound basis for administrators to analyze the network situation and prevent network attacks.

The vFW supports management from the H3C IMC management system, which collects and analyzes security information, and offers an intuitive view into network and security conditions, saving management efforts and improving management efficiency.

Wide range of authentication options

The vFW provides a wide range of authentication options to ensure access security.

Role-based access control

Assigns permissions based on user roles, which can prevent low-privileged users from obtaining or modifying configuration information.

Hierarchical view protection

Prevents low-level users from entering higher-level views.

Remote Authentication Dial-In User Service (RADIUS)

Cooperates with a RADIUS server to implement authentication, authorization, and accounting security services for access users to prevent unauthorized access.

PKI/X.509

Provides certificate-based authentication.

MD5 authentication in OSPF and RIP2

Ensures authenticity and integrity of exchanged routing information.

Rich VPN connection solutions

The vFW supports multiple VPN technologies for you to set up VPN connections as needed.

L2TP VPN

Sets up point-to-point tunnels across a public network (for example, the Internet) and transmits encapsulated PPP frames (L2TP packets) over the tunnels. L2TP is currently the most widely used Virtual Private Dial Network (VPDN) tunneling protocol. The vFW supports multiple L2TP multi-domains.

GRE VPN

EncGRE VPN—apsulates a protocol (such as IP, MPLS, or Ethernet) into a virtual point-to-point tunnel over a network (such as an IP network). Packets are encapsulated at one tunnel end and de-encapsulated at the other tunnel end.

IPsec VPN

Defined by the IETF to provide interoperable, high-quality, cryptography-based security for IP communications. IPsec uses Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols to ensure privacy, integrity, authenticity, and anti-replay of datagrams transmitted over the network. IPsec allows establishment of SAs automatically through Internet Key Exchange (IKE) or manually. The IPsec protocol provides a secure VPN solution for users who have high requirements for information security. IPsec VPN is typically used in combination with L2TP protocol and GRE protocol.

Technical specifications

Software specifications

Item	Description
Software image	H3C SecPath vFW1000 software image in ISO, OVA, QCOW2, or IPE format

Item	Description
Hypervisor	VMware ESXi Linux KVM H3C CAS
VM resources	A minimum of 1 vCPU (above 2.0 GHz clock speed) A minimum of 1 GB memory A minimum of 8 GB drive 2 to 16 vNICs, vNIC types: E1000, VMXNET3, VirtIO, and Intel 82599VF
Ethernet	Layer 3 Ethernet interface/subinterface, Layer 2 Ethernet interface ARP 802.1Q VLAN, VLAN termination PPPoE client
IP routing	Static routing Dynamic routing: RIPv1/v2, OSPFv2, BGP Routing policy
IP services	Forwarding/fast forwarding TCP, UDP, IP Option, IP unnumbered PBR Ping, tracer DHCP server, DHCP relay, DHCP client DNS client, DNS proxy, DDNS FTP server, FTP client, TFTP client Telnet server, Telnet client NTPv3/NTPv4/SNTPv3/SNTPv4 AFT SSHv1.5/2.0, SSL
IPv6	IPv6 ND, IPv6 PMTU, IPv6 FIB, IPv6 ACL IPv6 over IPv4 manual tunneling, automatic IPv4-compatible IPv6 tunneling, 6to4 tunneling, ISATAP tunneling Static routing Dynamic routing: RIPng, OSPFv3, BGP4+ IPv6 packet filtering IPv6 ASPF IPv6 interzone policy IPv6 attack defense

Item	Description	
AAA	Portal authentication RADIUS authentication HWTACACS authentication PKI/CA (X509 format) authentication Domain authentication CHAP authentication PAP authentication	
Firewall	Security zone, packets from a different security zone denied by default Defending against various malicious attacks, including land, smurf, fraggle, ping of death, teardrop, IP spoofing, IP fragmentation, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, address/port scanning, SYN flood, ICMP flood, and UDP flood Basic and advanced ACLs Interface-based ACLs Time range-based ACLs Dynamic packet filtering ASPF application layer packet filtering Static and dynamic blacklist MAC-IP binding MAC-based ACL Connection limit FIPS/CC mode	
NAT	Many-to-one NAT, which maps multiple internal addresses to one public address Many-to-many NAT, which maps multiple internal addresses to multiple public addresses One-to-one NAT, which maps one internal address to one public address NAT of both source address and destination address External hosts access to internal servers Internal address to public interface address mapping NAT support for DNS Setting effective period for NAT NAT ALGs for NAT ALG, including DNS, FTP, TFTP, PPTP, H.323, SIP, RSH, ILS, MSN, NBT	
VPN	L2TP VPN	Initiating a tunneling request to the LNS with the complete VPN username and the ISP domain name to which the user belongs. IP assignment to VPN users CHAP authentication to reauthenticate users and LCP renegotiation

Item	Description	
	IPsec/IKE	AH, ESP Setting up a security association automatically through IKE or manually Multiple ESP encryption algorithms including DES, 3DES, and AES MD5 and SHA-1 authentication algorithms IKE main-mode and aggressive-mode NAT traversal DPD
	GRE VPN	-
QoS	Traffic classification based on port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, or protocol type Congestion management: FIFO, WFQ, CBQ Congestion avoidance: Tail drop, WRED	
DC	VXLAN, OpenFlow1.3	
High availability	VRRP/VRRPv3 BFD Reth IRF	
Management and maintenance	User access management: console port, AUX port, SSH, Telnet, FTP Local management: CLI, automatic configuration, file system Network management: SNMPv1/v2c/v3, IMC, MIB, TR069, H3C IMC security management center, NETCONF Network monitoring: SNMPv1/v2c/v3, RMON, Syslog, NQA, sFlow, track, NetStream, EAA Others: Tcl, Python	

Performance specifications

Performance of software product is influenced by hardware and IO mode. The following performance references are only for reference.

CAS + SR-IOV

Item	1 × vCPU & 2G memory	4 × vCPUs & 8G memory	8 × vCPUs & 16G memory
FW throughput	9Gbps	37Gbps	45Gbps
Threat protection	1.6Gbps	7Gbps	16Gbps
IPSec VPN throughput	960Mbps	1.9Gbps	5Gbps

Item	1 × vCPU & 2G memory	4 × vCPUs & 8G memory	8 × vCPUs & 16G memory
Concurrent sessions	1.2 million	8 million	14 million
Threat protection throughput(APP+IPS+AV+URL)	800Mbps	1.2Gbps	2.5Gbps

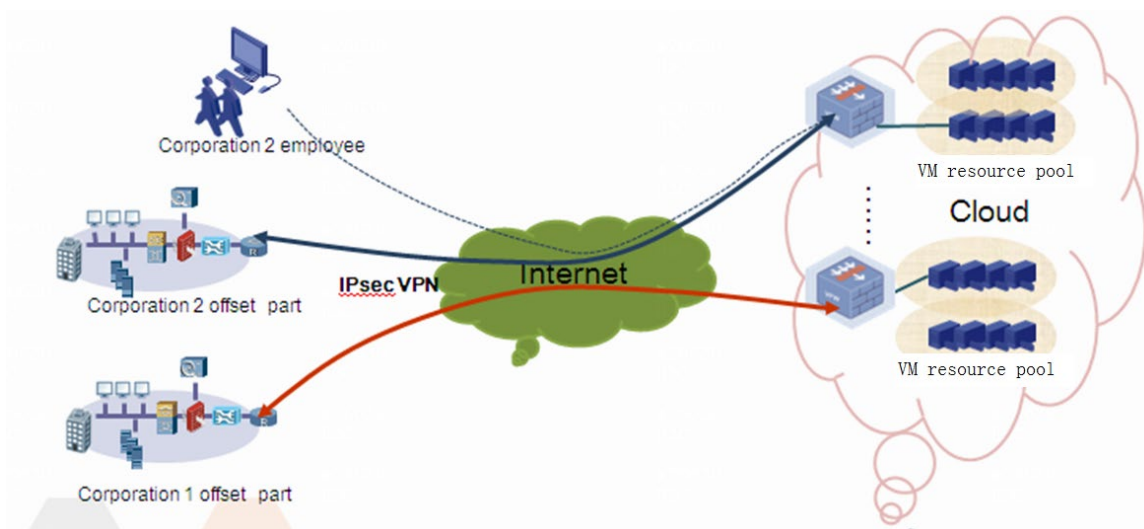
CAS + VIRTIO

Item	1 × vCPU & 2G memory	4 × vCPUs & 8G memory	8 × vCPUs & 16G memory
FW throughput	1.2Gbps	2.5Gbps	5Gbps
IPSec VPN throughput	500Mbps	1Gbps	2Gbps
Concurrent sessions	120 thousand	8 million	14 million
New sessions per second	20 thousand	60 thousand	120 thousand

Application scenarios

Tenant gateway in data centers

In the data center environment, the vFW can be used as a tenant gateway to provide secure access over VPN tunnels for different tenants and prevent all kinds of external attacks. It can also be used as an intranet access control device to isolate zones with different security levels and provide security protection for network traffic.



vFW as a tenant gateway networking

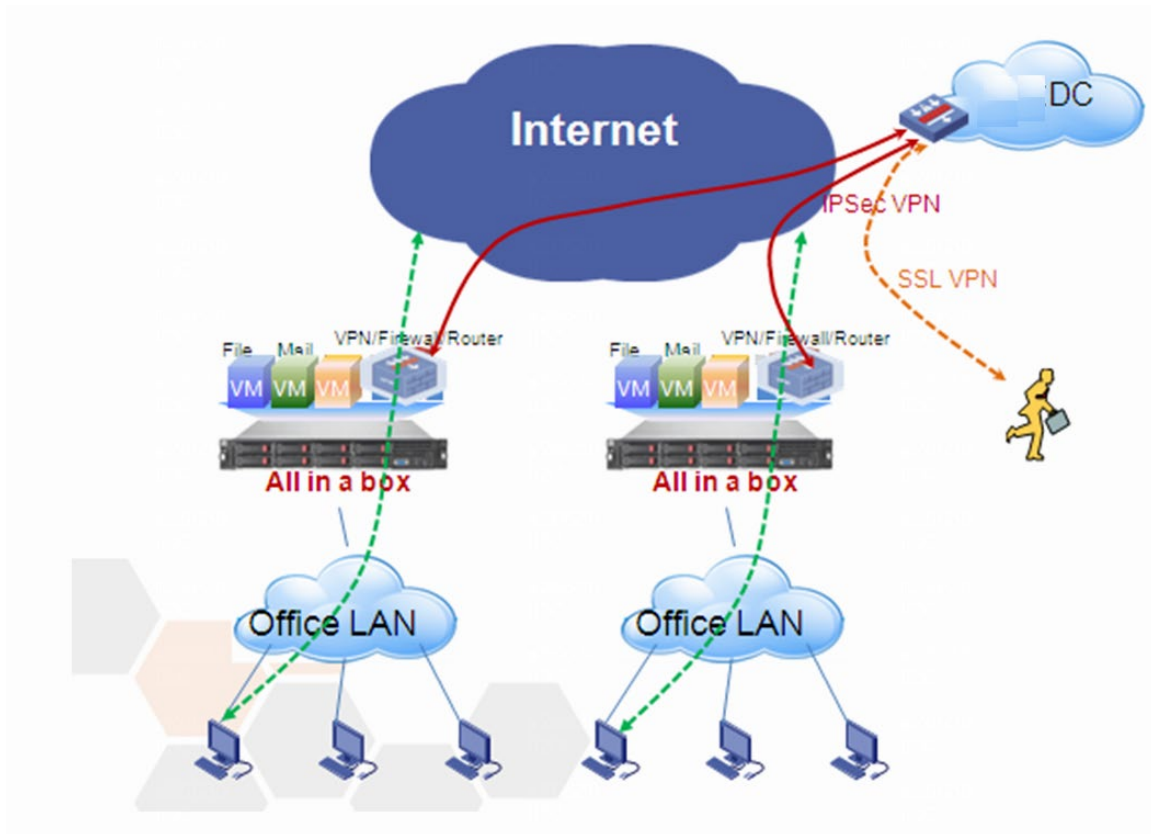
The vFW offers the following benefits as a tenant gateway in the data center environment:

- Deployed directly on a server, simplifying the network infrastructure and facilitating tenant maintenance.
- Elastic service scaling, dynamic performance adjustment, and highly efficient management.
- Security control by zone.
- NAT and ALG for multiple applications.
- Intrusions detection and prevention.
- Multiple attack defense technologies.
- Denylist filtering.
- SYN flood attack prevention through TCP proxy.
- Traffic logs and attack alarm logs.

Comprehensive gateway for enterprise branches

The vFW can be deployed at an enterprise branch to provide comprehensive gateway services. It delivers the following benefits:

- Deployed on a standard server, simplifying the network infrastructure and facilitating management.
- Provides Internet access and can establish VPN connections (including IPsec VPN, L2TP, and GRE) with the enterprise data center to ensure access security.
- Provides robust security protection for the branch.
- Deployed on the same hardware platform with enterprise applications, enabling computing and networking convergence.



vFW as an enterprise branch gateway networking

Ordering information

Item		Description
vFW1000 licenses	LIS-vFW1000-C1-Y1	H3C SecPath vFW1000 License (Comware V7, 1 vCPU, 1 Year)
	LIS-vFW1000-C1-Y3	H3C SecPath vFW1000 License (Comware V7, 1 vCPU, 3 Years)
	LIS-vFW1000-C1	H3C SecPath vFW1000 License (Comware V7, 1 vCPU, Permanent)
	LIS-vFW1000-C4-Y1	H3C SecPath vFW1000 License (Comware V7, 4 vCPUs, 1 Year)
	LIS-vFW1000-C4-Y3	H3C SecPath vFW1000 License (Comware V7, 4 vCPUs, 3 Years)
	LIS-vFW1000-C4	H3C SecPath vFW1000 License (Comware V7, 4 vCPUs, Permanent)
	LIS-vFW1000-C8-Y1	H3C SecPath vFW1000 License (Comware V7, 8 vCPUs, 1 Year)
	LIS-vFW1000-C8-Y3	H3C SecPath vFW1000 License (Comware V7, 8 vCPUs, 3 Years)
	LIS-vFW1000-C8	H3C SecPath vFW1000 License (Comware V7, 8 vCPUs, Permanent)
SSL VPN licenses	LIS-NFV-SSL-25	H3C NFV Feature License (Comware V7, SSL VPN, 25 Users)
	LIS-NFV-SSL-100	H3C NFV Feature License (Comware V7, SSL VPN, 100 Users)

Item		Description
	LIS-NFV-SSL-500	H3C NFV Feature License (Comware V7, SSL VPN, 500 Users)
	LIS-NFV-SSL-1000	H3C NFV Feature License (Comware V7, SSL VPN, 1000 Users)



New H3C Technologies Co., Limited
Beijing Headquarters
Tower 1, LSH Center, 8 Guangshun South Street,
Chaoyang
District, Beijing, China
Zip: 100102
Hangzhou Headquarters
No.466 Changhe Road, Binjiang District, Hangzhou,
Zhejiang,
China Zip: 310052
Tel: +86-571-86760000
Fax: +86-571-86760001

Copyright ©2025 New H3C Technologies Co., Limited
Reserves all rights Disclaimer: Though H3C strives to
provide accurate information in this document, we
cannot guarantee that details do not contain any
technical error or printing error. Therefore, H3C cannot
accept responsibility for any inaccuracy in this
document. H3C reserves the right for the modification
of the contents herein without prior notification.

<https://www.h3c.com>