SVN5800 Secure Access Gateway

SVN5800 Secure Access Gateway

SVN5850 / SVN5830 Secure Access Gateway

SVN5880 / SVN5860 Secure Access Gateway

Product Overview

The SVN5800 is the newest security access gateway of Huawei. Built on years of R&D and design experience in communications and networking, the SVN uses a carrier-grade high-availability hardware platform and embedded secure real-time operating system and meets the demanding international certification standards. The SVN series provides secure solutions, such as remote access, mobile working, branch office interconnection, cloud access, and access through multimedia tunnels for enterprises, governments, and carriers.

Features

Powerful Secure Access Ability

- Supports a maximum of 50,000 concurrent users, one of the highest performance levels in the industry.
- Supports a wide range of operating systems, such as Android, Windows, iOS, Mac OS, Linux, Symbian, and BlackBerry.
- Supports up to 4 VPN access types: SSL, IPSec, GRE and L2TP.
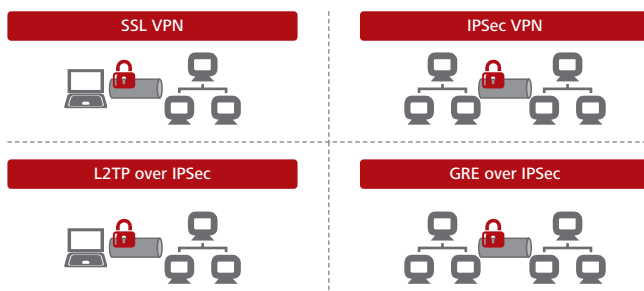
Holistic Security Protection

- Supports a wide variety of authentication and authorization methods, such as local password authentication, AD/LDAP, RADIUS, digital certificates, tokens, terminal ID, CAPTCHA code, USB key, or a combination of these methods to ensure security.
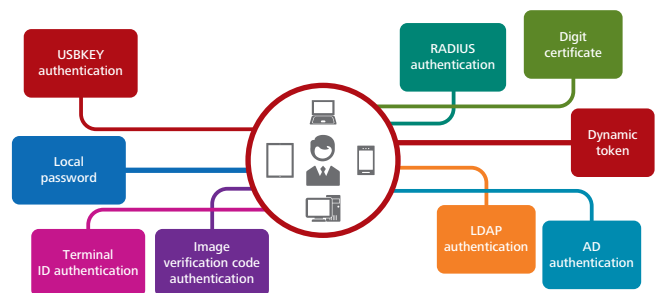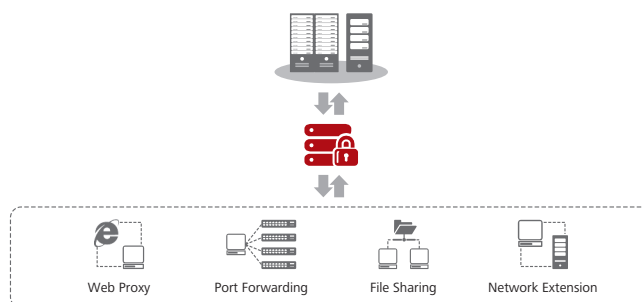

- Provides fine-grained access control based on application, IP address, port, and URL and is able to identify over 6000 application protocols.
- Supports host check, access history clearing, terminal ID binding, DDoS attack defense at application and network layers to ensure that devices can securely access the service resources and cannot be used as a jump-off point for attacks.
- The SVN uses the industry-leading virtual gateway technology and supports a maximum of 512 virtual SSL VPN gateways to reduce hardware investment. Each virtual SSL VPN gateway supports independent authentication, management, and configuration, which facilitates administrator operations, reduces maintenance costs, and allows for multiple virtual gateways on one physical gateway.
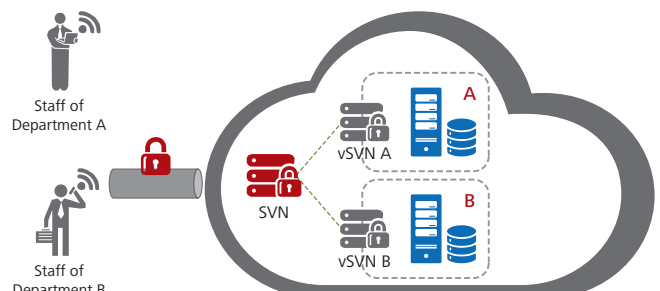
SVN5800 Secure Access Gateway

Agile Access Experience

- Supports a wide range of secure access methods, such as Web proxy, file sharing, port forwarding and network extension, for users to choose.
- Detects the best access gateway dynamically and chooses the best link automatically to ensure access experience.
- In the agile campus solution, the device can implement dynamically: User/user group-based traffic bandwidth management and control, prioritized login for VIP users, and hierarchical user access management to efficiently use enterprise network resources.

Web Proxy   Port Forwarding   File Sharing   Network Extension

Specifications

Model	SVN5830	SVN5850	SVN5860	SVN5880
Maximum number of concurrent SSL VPN users	6000	12,000	40,000	50,000
Maximum number of concurrent SSL VPN connections	15,000	30,000	150,000	150,000
IPSec VPN throughput	3Gbit/s	3Gbit/s	18Gbit/s	18Gbit/s
Concurrent IPSec VPN connections	4,000	4,000	15,000	15,000
Maximum number of virtual gateways	256	256	512	512
I/O				
Fixed ports	8GE+4SFP		4*10GE+16GE+8SFP	
Expansion slot	2WSIC		5WSIC	
Expansion card type	WSIC: 2×10GE (SFP+) +8×GE (RJ45), 8×GE (RJ45), 8×GE (SFP), 4×GE (RJ45) BYPASS			
Complete machine specifications				
Form Factor	1U		3U	
Dimensions (H×W×D) mm	442×421×43.6		442×415×130.5	
Weight (fully configured)	10KG		22KG	
HDD	Optional, 300 GB hot-swappable single hard disk		Optional, 300 GB hot-swappable dual hard disk (RAID1), supports hot swap	
Redundant power supply	Optional		Standard option	
AC power supply	100~240V			
Maximum power	170W		350W	700W
Operating environment	Temperature: 0°C to 45°C (without hard disk)/5°C to 40°C (with hard disk), humidity: 10% to 90%			
Non-operating environment (storage environment)	Temperature: -40°C to 70°C, humidity: 5% to 95% (non-condensing)			
Feature				
SSL VPN	Supports Web proxy, file sharing, port forwarding, network extension Supports resources such as Web, Client/Server application program, in IPv4 or IPv6			
VPN type	SSL, IPSec, GRE, L2TP			
User authentication	Supports local password (VPNDB), AD, RADIUS, LDAP, and SecurID authentication. Supports x.509 digital certificate, USB key certificate, terminal ID, and CAPTCHA authentication. Supports hierarchical certification, single sign-on, and the soft keyboard functions.			
Authentication control	Supports role-based authorization, external group mapping authorization, and dynamic authorization based on the security level of the terminals. Provides fine-grained access control based on application, IP address, port, and URL and is able to identify over 6000 application protocols.			
Supported operating systems	Supports Android, Windows, Mac OS, iOS, Linux, Symbian, and BlackBerry OS.			
Terminal security	Supports terminal/host security check, cache cleaning, terminal ID binding			
Virtual gateway:	Supports multiple virtual gateways on one physical gateway to allow for service and network virtualization and independent authentication, authorization, services, and resources management			
Agile feature	Bandwidth management, intelligent uplink selection			
Network security	Supports access control, NAT, and attack defense.			
Network protocols	Supports IPv4 and IPv6			
Deployment and availability	Supports transparent, routing, and hybrid deployment modes and active/standby high availability (HA)			

General Disclaimer

HUAWEI TECHNOLOGIES CO., LTD.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808
Version No.: M3-032102-20161220-C-1.0

www.huawei.com