SVN5800 Secure Access Gateway

The development of networks allows enterprises to provide remote access to branch offices, partners, customers, mobile employees, and home offices so that they can access application and data resources, such as OA, ERP, CRM, and SCM, on enterprise intranet. The access networks are complex. Some access networks, such as branch office and partner networks, can be managed by the enterprise. Some access networks, such as home, public Wi-Fi, and 3G networks, are geographically dispersed and out of the control of the enterprise. Moreover, the devices that access the enterprise intranet are diversifying. In addition to traditional terminals, such as desktop computer and laptops, smart devices are increasingly used to access enterprise networks. To facilitate business processing, enterprises must ensure that legitimate users can easily access information resources on the intranet from various devices on various networks, without compromising intranet security.

SVN5800 products are the latest secure access gateway products, which are built on a carrier-class hardware platform, secure real-time embedded operating system, and many years of experience in communication and networking development and design. SVN5800 products meet demanding international certification standards to provide security solutions, such as remote access, mobile working, branch office interconnection, cloud access, and multimedia tunnel access.

SVN5800 series secure access gateways

Product Features and Benefits

Anywhere Access

Powerful access capability

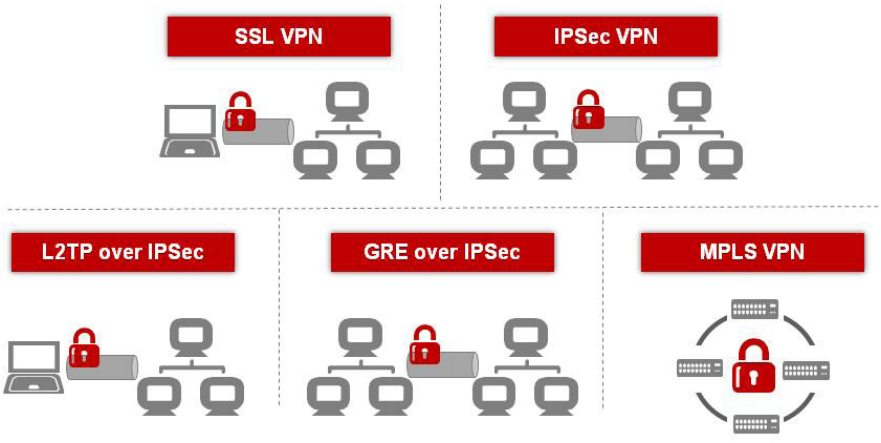
Support up to 100,000 concurrent users. This capacity is industry leading. The SVN5800 series secure access gateways use a hardware platform that has a brand new architecture, dedicated multi-core platform, and multiple CPUs for parallel processing.

Cross-OS support

The SVN5800 series secure access gateways support Android, Windows, iOS, Mac OS, Linux, Symbian, and BlackBerry operating systems.

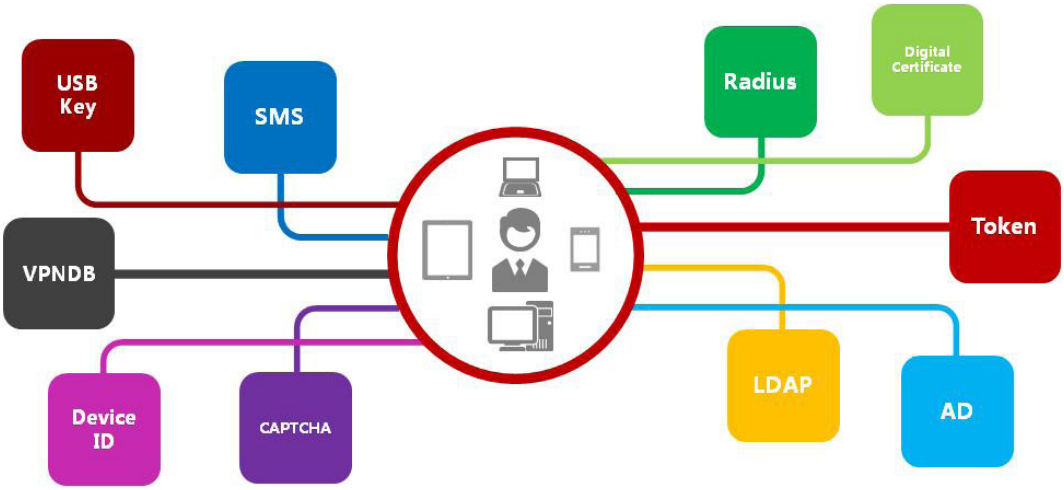
Full VPN support

The SVN5800 series secure access gateways support SSL, IPSec, GRE, L2TP, and MPLS VPN types.



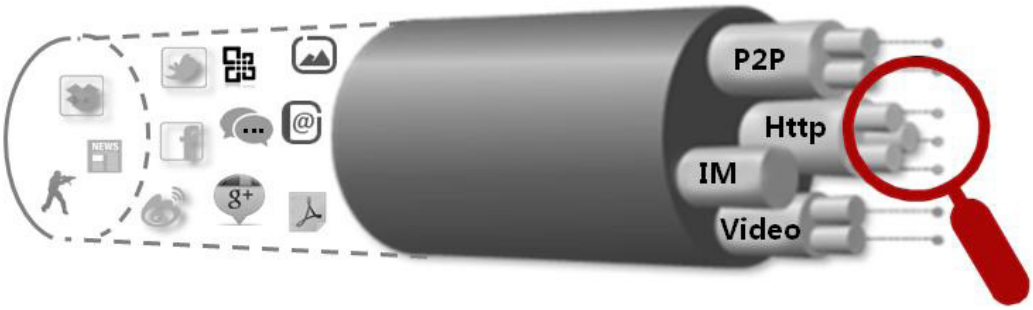
Secure Access

Diverse authentication types



The SVN5800 series supports authentication types, such as local password (VPNDB), AD/LDAP, RADIUS, digital certificate, token, USB key, short message service (SMS), device ID, and CAPTCHA. Therefore, the SVN5800 series allows you to combine multiple authentication factors so that users must pass the authentication of all configured authentication types to improve security. You can also configure multiple authentication types and allow users to gain VPN access if they pass any one of the configured authentication types.

Fine-grained security control



The SVN5800 series provides fine-grained access control based on application, IP address, port, and URL and is able to identify over 6000 application protocols.

The application-based access control allows you to permit the traffic of some applications, such as ERP and web, but limit or block the traffic of other applications, such as video and social networking applications. Such access control allows you to implement fine-grained traffic control to ensure that enterprise bandwidth resources are productively used.

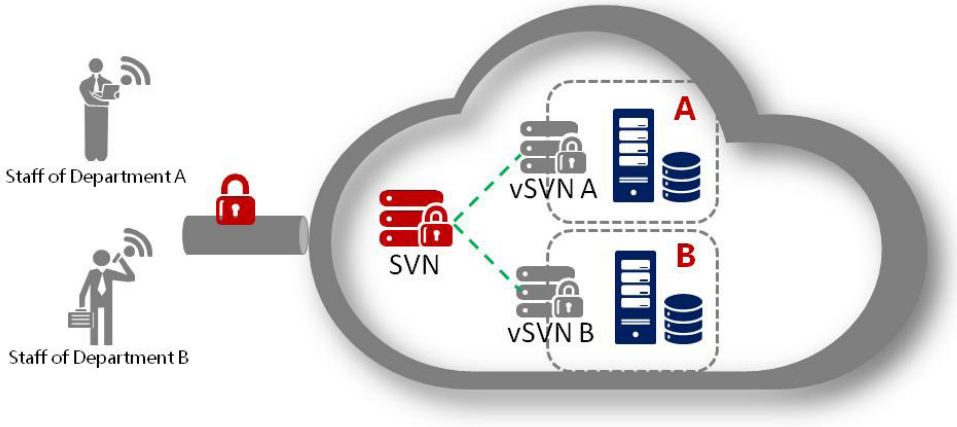
Comprehensive protection

The SVN5800 can check the security state of devices to determine whether to limit the resources accessible to the user or prevent the user from logging to the SVN to ensure that only secure devices can access the enterprise intranet. After the user logs out, the SVN5800 can delete access history, such as temporary files and cookies, to avoid data loss.

The SVN5800 series can also identify and prevent tens of attacks based on the traffic features and DDoS attack methods to ensure that user devices are not exploited to launch attacks.

Leading virtualization technologies

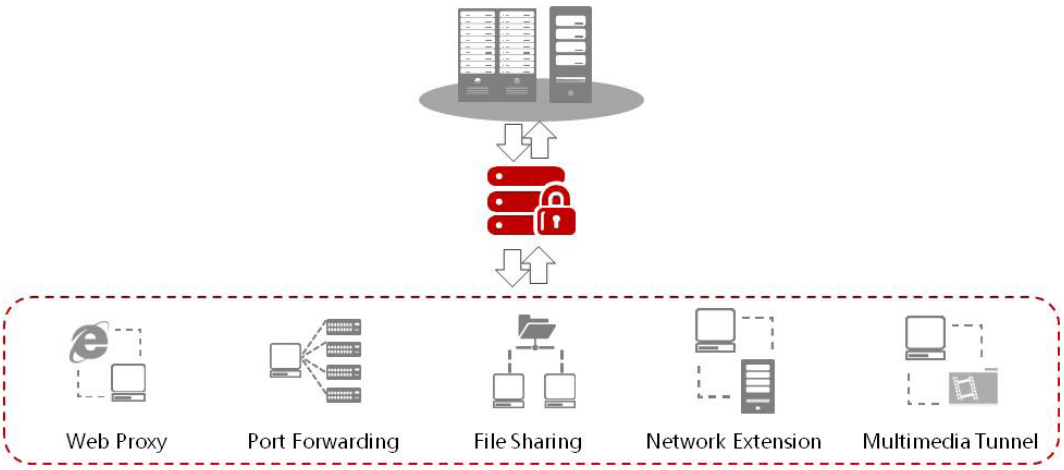
Up to 512 virtual SSL VPN gateways can be created on an SVN5800 secure access gateway. The virtual gateways are independent from each other and can be used by different enterprises of different departments of an enterprise. The virtual gateway technology maximizes device efficiency, minimizes hardware cost, and improve return on investment.



Agile Access

Flexible access methods

The SVN5800 supports secure access methods, such as Web proxy, file sharing, port forwarding, network extension, and multimedia tunnel.

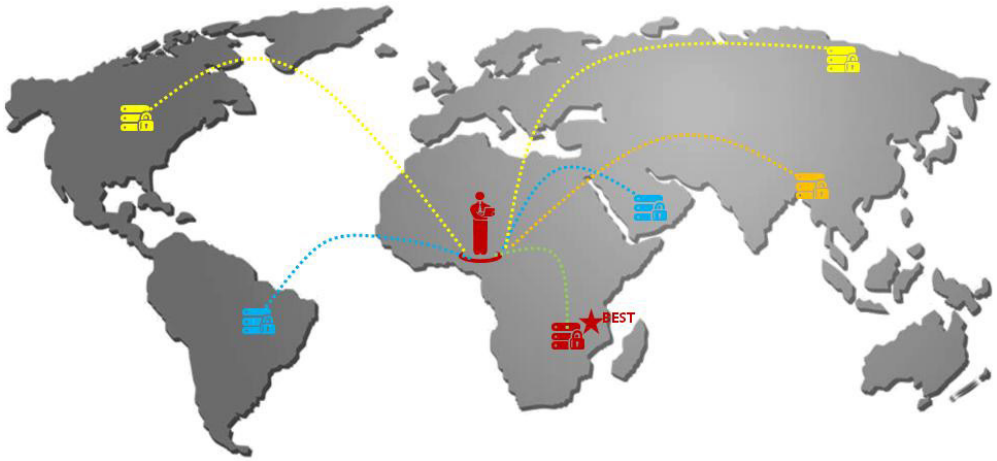


- Web proxy: When a remote user sends the SVN5800 a request for a web page hosted on the intranet, the SVN5800 forwards the request to the web server on the intranet, and sends the web page returned by the server to the user. The content of the web page is transmitted through SSL-encrypted tunnels to ensure data integrity.
- File sharing: The file systems on the intranet are put on the web so that users can user their browser to create and view folders and upload, download, rename, and delete files, just as they do on file systems. The SVN supports the SMB/CIFS and NFS protocols to provide secure remote access to Windows and Linux file systems, respectively.
- Port forwarding: Uses SSL to protect TCP applications and controls the access to these applications. A control is installed on the client to relay TCP/UDP services, encrypt data flows using SSL, and transmit the data flows to the SVN. Then, the SVN decrypts and parses the data flows and transmits the data flows to corresponding application servers, ensuring application security.
- Network extension: Provides remote access to network layer applications and resources by using Layer 3 SSL VPN (L3VPN) or IPSec Layer 3 VPN (IPSec L3VPN).
- Multimedia tunnel: By integrating the multimedia tunnel client component, multimedia clients can encrypt multimedia content using SSL tunnels, which have inherent advantages in traversing NAT and firewalls.

Intelligent ISP link selection

If multiple ISP links exist, the SVN5800 series can intelligently select an optimal ISP link to avoid the delay caused by cross-carrier routes.

If geographically dispersed secure access gateways are deployed, the SVN5800 allows clients to constantly probe gateway distribution and quality to select the fastest SVN gateway to access.



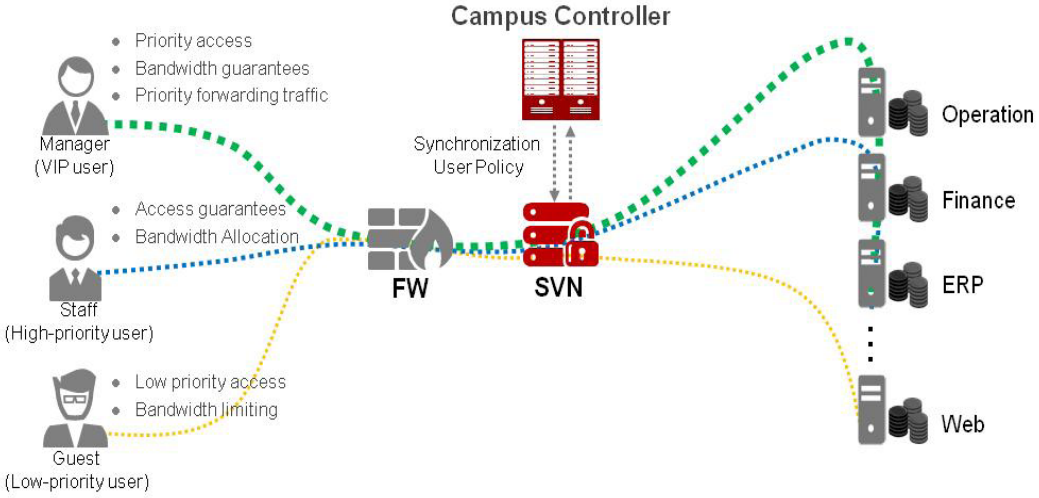
Service mobility*

The SVN5800 in the agile campus solution ensures that users can have the same network permissions, policies, and access experience regardless of users' location and IP addresses.

SVN user rate limiting: Bandwidth thresholds for SVN users are centrally configured on the controller. After SSL VPN users are authenticated, the controller delivers the bandwidth thresholds to users.

VIP access: If the users connected to a gateway reach the maximum capacity and a VIP user attempts to access the SVN, the SVN logs out some common users to ensure the access of the VIP user.

VIP traffic forwarding: User priorities are mapped to traffic priorities to ensure that the traffic of higher-priority users is forwarded preferentially.



Specifications

Device specifications

Model	SVN5830	SVN5850	SVN5860	SVN5880
Maximum number of concurrent SSL VPN users	6000	12,000	40,000	50,000 / 100,000*
Maximum number of concurrent SSL VPN connections	15,000	30,000	150,000	150,000
IPSec VPN throughput	3 Gbit/s	3 Gbit/s	18 Gbit/s	18 Gbit/s
Concurrent IPSec VPN connections	4000	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 slots	2WSIC		5WSIC	
Expansion card types	WSIC: 2x10GE (SFP+) + 8xGE (RJ45), 8xGE (RJ45), 8xGE (SFP), 4xGE (RJ45) BYPASS			
Device Specifications				
Form Factor	1U		3U	
Dimensions (H x W x D) mm	43.6 x 442 x 421		130.5 x 442 × 415	
Weight (fully configured)	10 KG		22 KG	
HDD	Optional, 300 GB hot-swappable single hard disk		Optional, 300 GB hot-swappable dual hard disks (RAID1)	

Model	SVN5830	SVN5850	SVN5860	SVN5880
Redundant power supply	Optional		Standard	
AC power supply	100 V to 240 V			
Maximum power	170 W		350 W	700 W
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)			
Functions				
SSL VPN	Supports Web proxy, file sharing, port forwarding, network extension, and multimedia tunnel*. Supports access to resources, such as Web, Client/Server application program, and multimedia resources, in IPv4 or IPv6			
VPN types	SSL VPN, IPSec VPN, GRE VPN, L2TP VPN, MPLS VPN			
User authentication	Supports authentication methods, such as local password (VPNDB), AD, RADIUS, LDAP, SecurID, X.509 digital certificate, USB key, SMS, device ID, and CAPTCHA authentication. Supports hierarchical authentication, single sign-on (SSO), and software keyboard.			

Model	SVN5830	SVN5850	SVN5860	SVN5880
Authentication control	Supports role-based, external group mapping, 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, and DDoS attack defense at application and network layers*.			
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 ISP link 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/active and active/standby high availability (HA)			

* The product information may contain the product functions provided in future. For the actual product specifications, contact Huawei local sales office.