Vigor2950 Series

Dual WAN SSL VPN Appliance

DrayTek

www.draytek.com

- *Dual-WAN provides policy-based load-balancing and fail-over*
- *Content Security Management (CSM) strengthens appliance-based gateway security*
- *Robust firewall prevents external attacks and provides Internet access policies*
- *Hardware-based platform delivers high performance VPN*
- *Up to 200 simultaneous (IPSec/PPTP/L2TP) VPN channels*
- *VPN trunking (VPN load-balancing and backup)*
- *Up to 50 concurrent SSL VPN tunnels with LDAP/RADIUS authentication*
- *Flexible bandwidth management to optimize bandwidth usage*
- *USB port for 3.5G USB modem/printer (Vigor2955)*

The Vigor2950 series serves as a VPN gateway and a central firewall for multi-site offices and tele-workers. With its high data throughput of 90Mbps, Dual WAN, VPN trunking and 5 Gigabit LAN ports, the device facilitates productivity of versatile business operations. To secure communications between sites is the establishment of VPN tunnels up to 200 simultaneous tunnels.

High user-friendliness and efficiency

Its well-structured Web User Interface offers user-friendly configuration. The WUI also provides IP layer QoS (Quality of Service), NAT session/bandwidth management to help users control and allocate the bandwidth on networks.

More extendability

With a dedicated VPN co-processor, the hardware encryption of AES/DES/3DES and hardware key hash of SHA-1/MD5 are seamlessly handled, thus maintaining maximum router performance. For remote tele-workers and inter-office links, the Vigor2950 supports up to 200 simultaneous VPN tunnels (such as IPSec/PPTP/L2TP protocols) and 50 sessions of SSL VPN by using LDAP/RADIUS authentication.

Without the necessity of installing VPN client on individual PC, the Secure Socket Layer (SSL) virtual private network (VPN) facility lets remote workers connect to the office network at any time. SSL is supported by standard web browsers such as FireFox and IE. For users of small offices and tele-workers who need to access enterprises' internal applications, file server and file sharing, Vigor2950 security router series allow up to 50 concurrent SSL sessions.

Maximum degree of operational reliability

It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such as DSL, cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic can be guided and switched to the normal communication port for proper operation.

Security without compromise

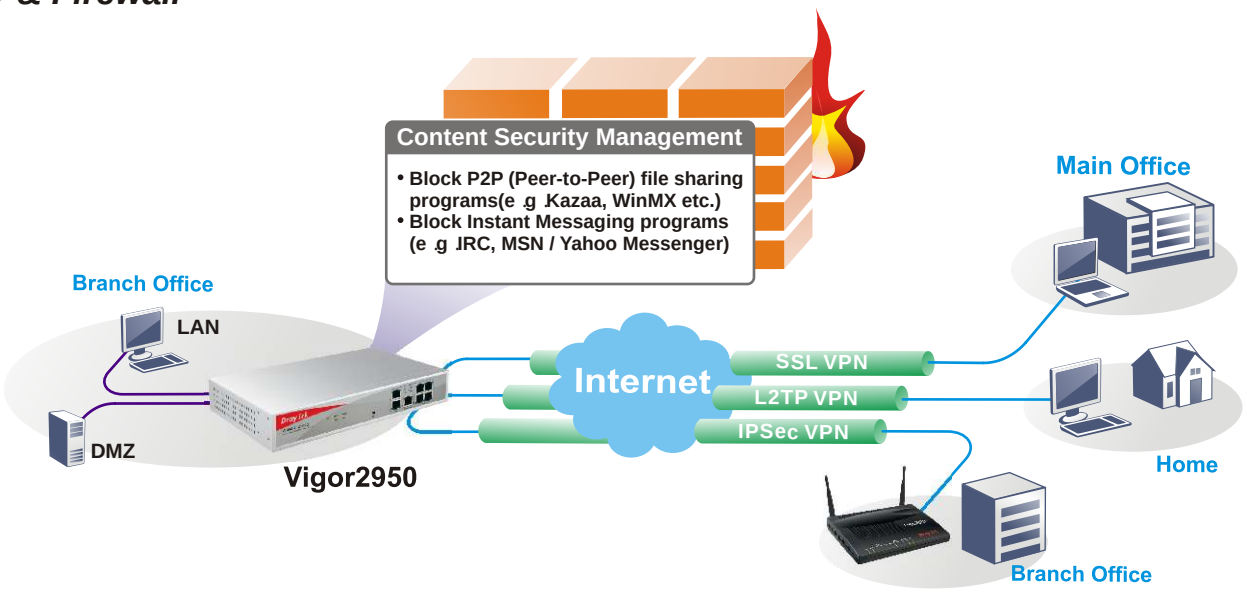
The Vigor2950 series also provides high-security firewall options with both IP-layer and content based protection. The DoS/DDoS prevention and URL/Web content filter strengthen the security outside and inside the network. The enterprise-level CSM (Content Security Management) enables users to control and manage IM (Instant Messenger) and P2P (Peer to Peer) applications more efficiently. The CSM hence prevents inappropriate content from distracting employees and impeding productivity. Furthermore, the CSM can keep office networks threat-free and available. With CSM, you can protect confidential and essential data from modification or theft.

More benefits

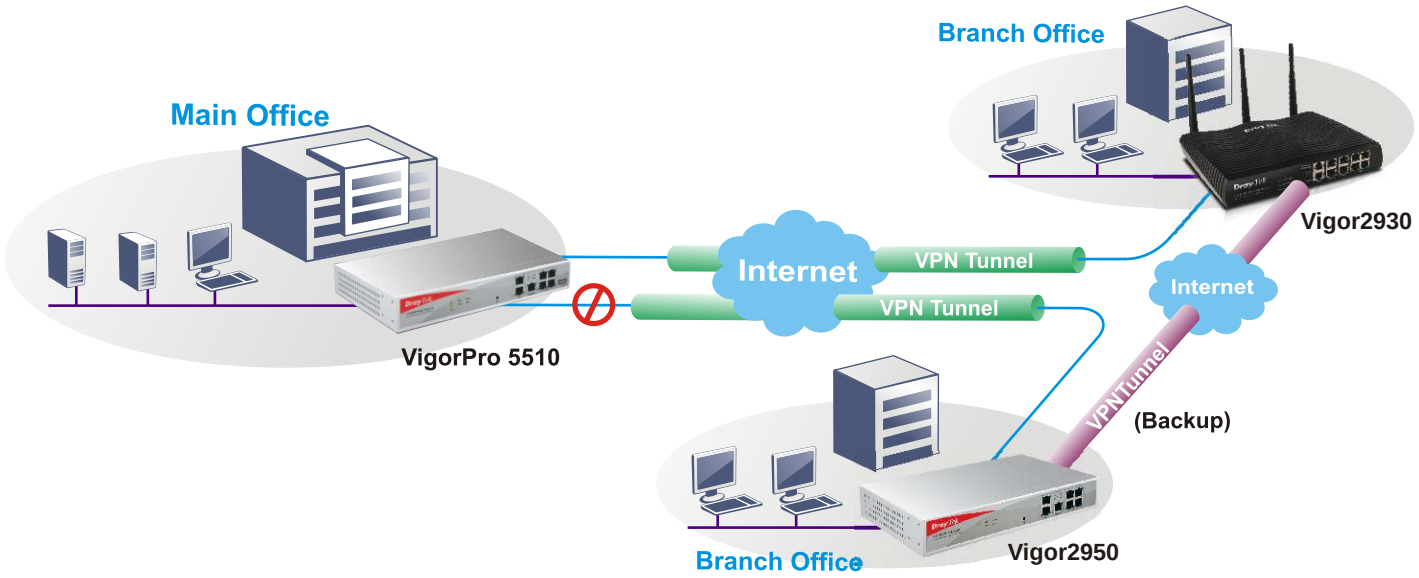
With high-performance Super G™ wireless connectivity, the router enables the wireless access rate up to 108Mbps. Besides the encryption methods of WEP/WPA/WPA2 and MAC address control, it also offers wireless LAN isolation, wireless VLAN and 802.1X authentication. WDS (Wireless Distribution System) can help users extend wireless coverage easily. Moreover, the wireless rate control can adjust the connection rate of each wireless station. The ISDN interface can offer remote access or dial-backup.

Dual-WAN | SSL VPN | Smart Monitor | CSM | P2P | Network Management

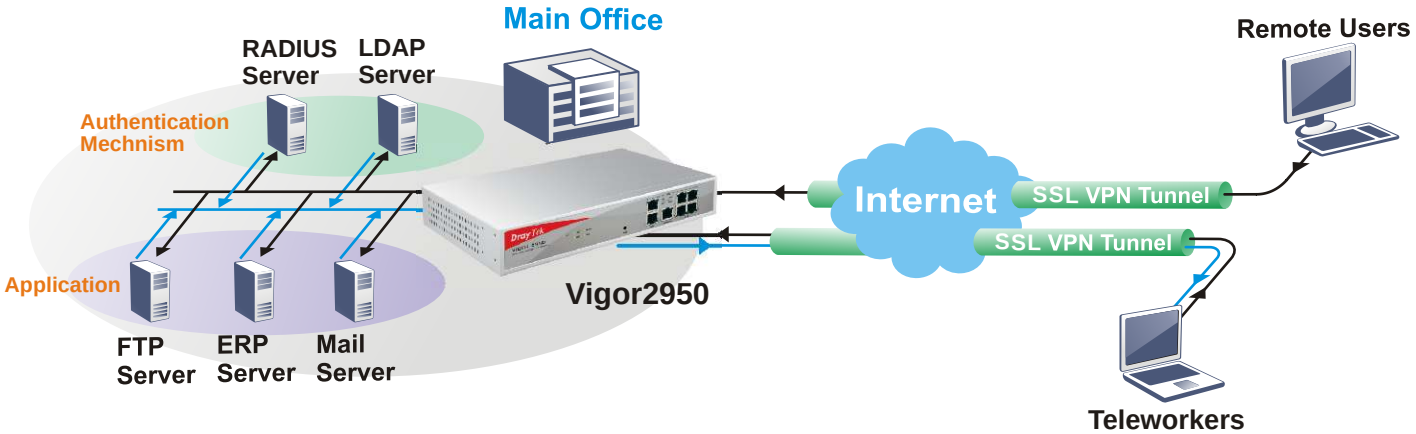
Security & Firewall



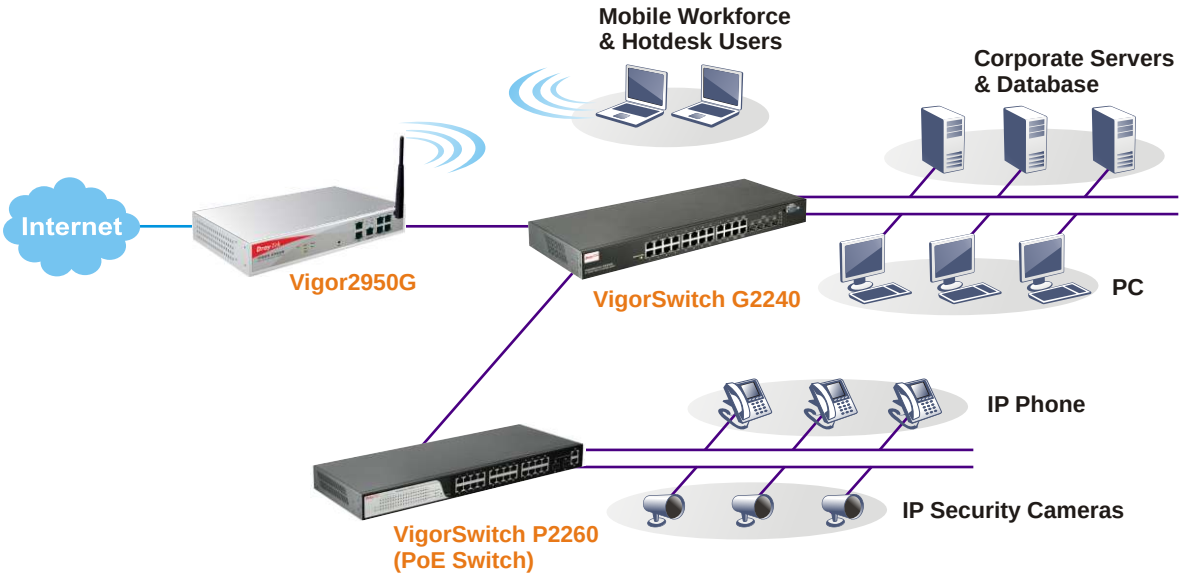
VPN Trunking



SSL VPN with LDAP/RADIUS authentication



Extendability



Vigor2950 Dual WAN

New DrayOS Version 3 Operating System including new object-based Firewall

WAN Protocol

Ethernet	• PPPoE, PPTP, DHCP client, static IP, L2TP, BPA
ISDN	• DSS1 (Euro ISDN), PPP, ML-PPP(64/128Kbps)

Dual WAN

Outbound Policy Based Load Balance	• Allow your local network to access Internet using multiple Internet connections with high-level of Internet connectivity availability • Two dedicated Ethernet WAN ports (10/100Mb/s) • WAN fail-over or load-balanced connectivity
Bandwidth on Demand	• Service/IP based preference rules or auto-weight

VPN

Protocols	• PPTP, IPSec, L2TP, L2TP over IPSec
Up to 200 Sessions Simultaneously	• LAN to LAN, remote access (teleworker-to-LAN), dial-in or dial-out
VPN Trunking	• VPN load-balancing and VPN backup
SSL VPN	• Allow users to use a web browser for secure remote user login tunnel mode, application mode, proxy mode
LDAP	• Lightweight directory access protocol. The enterprises use LDAP authentication technology to allow administrator, IT personnel and users to be authenticated when trying to access company's intranet environment.
VPN Throughput	• 50Mbps
NAT-Traversal (NAT-T)	• VPN over routes without VPN pass-through
PKI Certificate	• Digital signature (X.509)
IKE Authentication	• Pre-shared key; IKE phase 1 aggressive/standard modes & phase 2 selectable lifetimes
Authentication	• Hardware-based MD5, SHA-1
Encryption	• MPPE and hardware-based AES/DES/3DES
RADIUS Client	• Authentication for PPTP remote dial-in
DHCP over IPSec	• Because DrayTek add a virtual NIC on the PC, thus, while connecting to the server via IPSec tunnel, PC will obtain an IP address from the remote side through DHCP protocol, which is quite similar with PPTP
Dead Peer Detection (DPD)	• When there is traffic between the peers, it is not necessary for one peer to send a keep-alive to check for liveness of the peer because the IPSec traffic serves as implicit proof of the availability of the peer.
Smart VPN Software Utility	• Provided free of charge for teleworker convenience (Windows environment)

Easy of Adoption	• No additional client or remote site licensing required
Industrial-standard Interoperability	• Compatible with other leading 3rd party vendor VPN devices

Content Filter

URL Keyword Blocking	• Whitelist and Blacklist • Java applet, cookies, active X, compressed, executable, multimedia file blocking
Web Content Filter	• Dynamic URL filtering database
Time Schedule Control	• Set rule according to your specific office hours

Firewall

Stateful Packet Inspection (SPI)	• Outgoing/Incoming traffic inspection based on connection information
Content Security Management(CSM)	• Appliance-based gateway security and content filtering
Multi-NAT	• You have been allocated multiple public IP address by your ISP. You hence can have a one-to-one relationship between a public IP address and an internal/private IP address. This means that you have the protection of NAT (see earlier) but the PC can be addressed directly from the outside world by its aliased public IP address, but still by only opening specific ports to it (for example TCP port 80 for an http/web server).
Port Redirection	• The packet is forwarded to a specific local PC if the port number matches with the defined port number. You can also translate the external port to another port locally.
Open Ports	• As port redirection (above) but allows you to define a range of ports.
DMZ Host	• This opens up a single PC completely. All incoming packets will be forwarded onto the PC with the local IP address you set. The only exceptions are packets received in response to outgoing requests from other local PCs or incoming packets which match rules in the other two methods. The precedence is as follows : Port Redirection > Open Ports > DMZ
Policy-based IP Packet Filter	• The header information of an IP packet (IP or MAC source/destination addresses; source /destination ports; DiffServ attribute; direction dependent, bandwidth dependent, remote-site dependent
DoS/DDoS Prevention	• Act of preventing customers, users, clients or other computers from accessing data on a computer.
IP Address Anti-spoofing	• Source IP address check on all interfaces:only IP addresses classified within the defined IP networks are allowed.
Object-based Firewall	• Utilizes object-oriented approach to firewall policy
Notification	• E-mail alert and logging via syslog
Bind IP to MAC Address	• Flexible DHCP with 'IP-MAC binding'
WDS Security	• The use of authentication and encryption techniques on a Wireless Distribution System (WDS) link between compatible access points.

Wireless Access Point

Wireless VLAN (Wireless LAN Isolation)	• Blocks users in a VLAN from sending traffic directly to each other.
MAC Address Access Control	• Authorizes a defined IP user to use WLAN; this is used by the LAN to identify each client uniquely in order to switch packets correctly.
VPN over WLAN	• Create a secure tunnel between wireless client PC and the router, over the existing wireless connection, thus providing greater security as the traffic between that wireless client and the router is then encrypted and within a private tunnel using IPSec/3DES encryption (or as selected)
64/128-bit WEP	• WEP (Wireless Encryption Protocol) is a method of data encryption for wireless clients, which makes the sending of your data over the wireless interface more secure. By default, WEP is turned off on the router.
Hidden SSID	• Prevent from Wireless sniffing
802.1X Authentication with RADIUS Client	• IEEE standard for port-based network access control. The authenticator acts like a security guard to a protected WLAN network.
WPA/WPA2	• An authentication/encryption standard from the WiFi Alliance; WPA is intended to replace WEP encryption, being considered to be more secure and is a pre-cursor to the eventual IEEE 802.11i standard.

Wireless Distribution System (WDS)	• Provides bridged traffic between two LANs through air. Extend the coverage of a WLAN
AP Discovery	• Scan all regulatory channels and find working access points in the neighbourhood. Users will know which channel is clean for usage.
Wireless Rate Control	• Manage upload/download rate of each VLAN or station

System Management

Web-based User Interface (HTTP/HTTPS)	• Integrated web server for the configuration of routers via Internet browsers with HTTP or HTTPS
DrayTek's Quick Start Wizard	• Let administrator adjust time zone and promptly set up the Internet (PPPoE, PPTP, Static IP, DHCP).
User Administration	• RADIUS user administration for dial-in access (PPP/PPTP and ISDN CLIP).
CLI(Command Line Interface, Telnet/SSH)	• Remotely administer computers via the telnet
DHCP Client/Relay/Server	• Provides an easy-to configure function for your local IP network.
Dynamic DNS	• When you connect to your ISP, by broadband or ISDN you are normally allocated an dynamic IP address. i.e. the public IP address your router is allocated changes each time you connect to the ISP. If you want to run a local server, remote users cannot predict your current IP address to find you.
Administration Access Control	• The password can be applied to authentication of administrators.
Configuration Backup/Restore	• If the hardware breaks down, you can recover the failed system within an acceptable time. Through TFTP, the effective way is to backup and restore configuration between remote hosts.
Port-based VLAN	• Create separate groups of users via segmenting each of the Ethernet ports. Hence, they can or can't communicate with users in other segments, as required.
Built-in Diagnostic Function	• Dial-out trigger, routing table, ARP cache table, DHCP table, NAT sessions table, wireless VLAN online station table, data flow monitor, traffic graph, ping diagnosis, trace route
NTP Client/Call Scheduling	• The Vigor has a real time clock which can update itself from your browser manually or more conveniently automatically from an Internet time server (NTP). This enables you to schedule the router to dial-out to the Internet at a preset time, or restrict Internet access to certain hours. A schedule can also be applied to LAN-to-LAN profiles (VPN or direct dial) or some of the content filtering options.
Firmware Upgrade via TFTP/ HTTP/FTP	• Using the TFTP server and the firmware upgrade utility software, you may easily upgrade to the latest firmware whenever enhanced features are added.
ISDN Remote Maintenance	• The system manager can remotely manage the routers through an ISDN remote dial-in with secure call back mechanism.
Remote Maintenance	• With Telnet/SSL, SSH (with password or public key), browser (HTTP/HTTPS), TFTP or SNMP, firmware upgrade via HTTP/HTTPS or TFTP.
Wake On LAN	• A PC on LAN can be woken up from an idle/stand by state by the router it connects when it receives a special 'wake up' packet on its Ethernet interface.
Logging via Syslog	• Syslog is a method of logging router activity.
SNMP Management	• SNMP management via SNMP V2 , MIB II

Bandwidth Management

Traffic Shaping	• Dynamic bandwidth management with IP traffic shaping
Bandwidth Reservation	• Reserve minimum and maximum bandwidths by connection based or total data through send/ receive directions
Packet Size Control	• Specify size of data packet
DiffServ Codepoint Classifying	• Priority queuing of packets based on DiffServ
4 Priority Levels(Inbound/Outbound)	• Prioritization in terms of Internet usage
Individual IP Bandwidth/Session Limitation	• Define session /bandwidth limitation based on IP address
Bandwidth Borrowing	• Transmission rates control of data services through packet scheduler
User-defined Class-based Rules	• More flexibility

Routing Functions

Router	• IP and NetBIOS/IP-multi-protocol router
Advanced Routing and Forwarding	• Complete independent management and configuration of IP networks in the device, i.e. individual settings for DHCP, DNS, firewall, VLAN, routing, QoS etc.

DNS	• DNS cache/proxy
DHCP	• DHCP client/relay/server
NTP	• NTP client, automatic adjustment for daylight-saving time
Policy-based Routing	• Based on firewall rules, certain data types are marked for specific routing, e.g. to particular remote sites or lines.
Dynamic Routing	• It is with routing protocol of RIP v2. Learning and propagating routes; separate settings for WAN and LAN.
Static Routing	• An instruction to re-route particular traffic through to another local gateway, instead of sending it onto the Internet with the rest of the traffic. A static route is just like a 'diversion sign' on a road.

ISDN Functionality

• ISDN TE interface • Layer 1 conforms to ITU-T1.430

Secure Call Back	• Access control. Consolidation and centralization of phone billing. Cost savings on toll calls.
Remote Activation	• Allows a remote user to make a phone call to a router and then ask router to dial up to the ISP.
Bandwidth on Demand	• As the ISDN BRI interface has two independent B channels, the BoD mechanism allows you to automatically add/drop a B channel according to data traffic throughput.
Remote Dial-in Access	• Allow remote users to utilize company's Internet resources and remote management.
Virtual TA	• This provides a 'CAPI' software interface, similar to that which an actual ISDN terminal adaptor installed on your PC might provide. This allows you to install CAPI-compliant software for dial-up networking, fax or voice activities - depending on the capabilities of your CAPI software. CAPI is only available on ISDN lines

Internet CSM (Content Security Management) Featuring

- URL keyword filtering - whitelist or blacklist specific sites or keywords in URLs
- Block web sites by category (subject to subscription)
- Prevent accessing of web sites by using their direct IP address (thus URLs only)
- Blocking automatic download of Java applets and ActiveX controls
- Blocking of web site cookies
- Block http downloads of file types (binary, compressed, multimedia)
- Time schedules & exclusions for enabling/disabling these restrictions
- Block P2P (Peer-to-Peer) file sharing programs (e.g. Kazaa, WinMX etc.)
- Block Instant messaging programs (e.g. IRC, MSN/Yahoo Messenger)

Hardware

LAN	• 5-port 10/100/1000 base-TX switch
WAN	• 2-port 10/100 base-TX ethernet
WLAN	• IEEE802.11b/g compliant, Super G™ 108Mbps (Vigor2950G /Gi)
ISDN	• 1-port with RJ-45 connector (Vigor2950i /Gi)
USB	• 1-port for 3.5G USB modem/printer (Vigor2955) USB 3.5G backup only for WAN1

Support

Smart Monitor (Free & Optional Utility)	• Network service analyze • User Management • System Management • User Analysis • Top10 ranking system • Up to 100 PC users
Warranty	• 2-year limited warranty, technical support through e-mail and internet FAQ/application notes
Firmware Upgrade	• Free firmware upgrade from Internet

Declaration of Conformity

CE FC

	ISDN	Wireless
Vigor2950Gi	●	●
Vigor2950G		●
Vigor2950i	●	
Vigor2950		
Vigor2955		

Green IT

www.draytek.com E-mail:info@draytek.com Tel:+886 3 597 2727 Fax:+886 3 597 2121