DrayTek

working with ACS SI

Vigor2960 Series

Dual-WAN Security Firewall

DrayTek Vigor2960 Series - Dual-WAN Security Firewall combines high-speed Internet access and comprehensive security through advance firewall and VPN designed for enterprise small branch offices and service provider. Vigor2960 Series with the powerful platform can manage concurrent services applications, ensure business continuity and protect investment.

Product Overview

The Vigor2960 Series serves as a VPN gateway and a central firewall for multi-site offices and tele-workers. With its high data throughput of two-Gigabit Ethernet, Dual WAN, VPN trunking and 4 Gigabit Ethernet 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.

DrayTek Vigor2960 Series - Dual-WAN Security Firewall offers:

- Gigabit Dual WAN interface providing load-balancing and failover for high performance and business continuity
- 4-port Gigabit LAN interface for facilitating managed services applications
- Enhanced security including:
  - Object-base firewall with advance users (e.g. IP), applications (e.g. IM & P2P,) and content management (web category, keyword and URL)
  - VPN connection for LAN-to-LAN (site-to-site) and Remote dial-in (client-to-site) with dynamic VPN services: IP Security (IPSec) VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES]), SSL VPN web proxy
- An 4-port 10/100/1000 Gigabit Ethernet managed switch with VLAN support (Up to 20 VLAN groups)
- Two USB 2.0 ports for printer, file sharing* and 3.5G/4G USB mobile broadband*
- Bandwidth Management with 8-level priority Inbound/Outbound QoS
- IPv4/IPv6 support to protect investment
- TR-069 Management / Working with VigorACS SI

*Firmware Upgradeable

Gigabit LAN / WAN | IPv6 Ready | VPN | CSM | Firewall | Bandwidth Management

Vigor2960 Series

Models	WAN 1	WAN 2	LAN Interface	Integrated USB 2.0
Vigor2960	Gigabit Ethernet (GE)		4-port 100/1000 managed switch	Yes
Vigor2960F	Fiber (SFP)	GE	4-port 100/1000 managed switch	Yes

Vigor2960 Series for Enterprise Small Branch-Office Deployment

Architecture Features and Benefits

Security without compromise

The Vigor2960 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.
By incorporating Commtouch's GlobalView™ URL Filtering services, DrayTek ensures its customers' networks are protected by the best available security technology.

Security
Enable real-time protection from emerging Web threats including malware, phishing and Zombies/bots

HR compliance/regulation
Prevent browsing to questionable content like pornography and hate sites

Productivity
Block or monitors sites to maximize employee productivity

Bandwidth regulation
Identify sites that consume an organization's bandwidth (e.g. movies, music)

Enterprise-level VPN Network

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 Vigor2960 supports up to 200 simultaneous VPN tunnels (such as IPSec/PPTP/L2TP protocols) and 100 sessions of SSL VPN. The Vigor2960 provides the Web Proxy based SSL encryption for tele-workers and/or remote access. 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, Vigor2960 security router series allows up to 100 concurrent SSL sessions.

Business Continuity

Note:
1. GE WAN 1 & 2 can do load balancing and backup.
2. VPN Trunk Management can do load balancing and backup.

More benefits

DrayTek has implemented IPv6 on Vigor2960 to ensure a smooth migration path for the affordable but faster broadband. The WAN-IPv6-connection can be established via Static IPv6, DHCPv6 and TSPC. There are two USB ports on Vigor2960. In addition to the function of USB printer server, you can connect a compatible 3.5G USB mobile for access to the cellular network. You can also add storage memory to the USB port of Vigor2960 in the form of a USB memory key or a USB hard drive. Then, the FTP access file uploading/downloading can be from the local LAN of Vigor2960 or from anywhere on the Internet*. It is very simple for you to deploy file depository. With user name and passwords, each of file depository can have their own directories and/or file access rights.

Features and Benefits of Vigor2960 Series

Feature	Benefit
Enable performance of concurrent services	• Powerful platform optimizes the broadband networks speeds while running multiple secure, concurrent services.
WAN interface: Gigabit Ethernet	• Dual WAN design for failover protections and load balancing.
4-port 100/1000 managed switch	• Facilitating managed services applications.
Enhanced security	• High-security firewall options with both IP-layer and content based protection. • Data privacy over the Internet via VPN (IPSec/PPTP/L2TP) with AES/DES/3DES encryption. • Content filtering via CSM protects confidential and essential data from modification or theft.
2 USB 2.0 ports	• Integrated USB ports can be configured to printer, file sharing* and 3.5G mobile broadband backup*.
TR-069 Central Management (VigorACS SI)	• Centrally manageable via VigorACS SI lowering TCO.

Working with TR-069 Central Management System

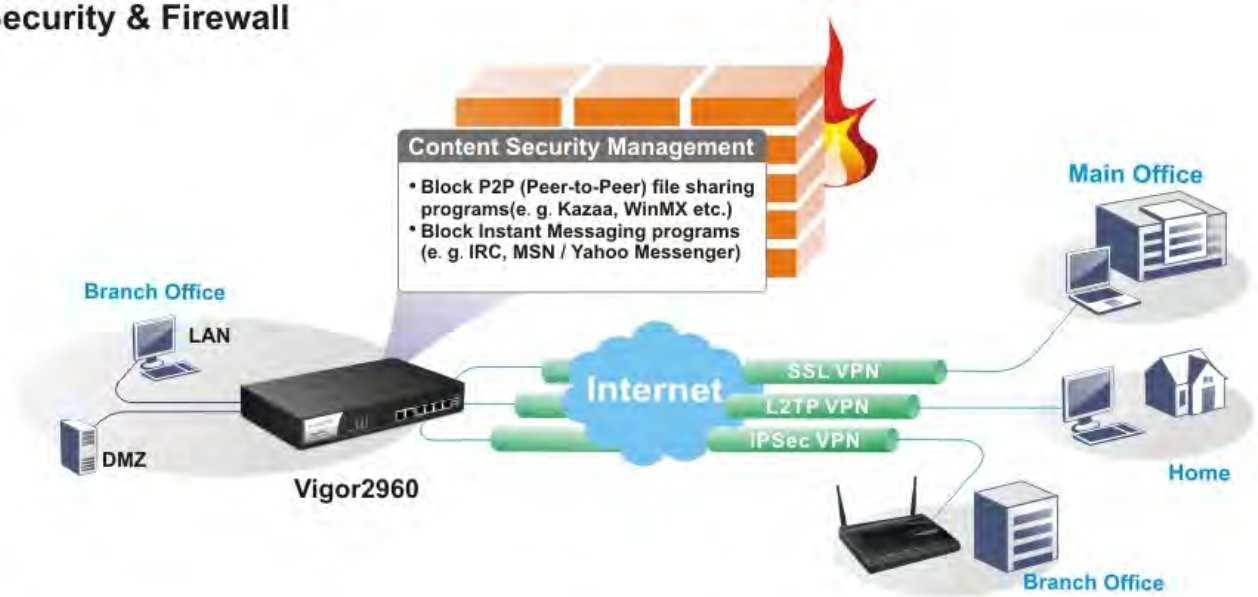
The Vigor2960 Series can be centrally managed by VigorACS SI to lower the workload of the IT Dept. The VigorACS SI centrally manages essential router features, such as LAN, WAN, WLAN or VoIP without the technician visits that improves user experience and contribute significant cost-saving. For instance, admin can schedule firmware or configuration updates for selected devices at one time. It also offers the real-time alert to notify admin when things go wrong, such as disconnected or VPN dropped via e-mail and SMS to guarantee the faster response.

Summary

Vigor2960 Series - Dual-WAN Security Firewall delivers state-of-the-art security and performance which allows enterprise small branch-office customers to optimize the usage of the high-speed broadband access. Managed service provider and system integrator can install Vigor2960 Series to give business customers a complete network solution in their remote sites.

*Firmware Upgradeable

Security & Firewall



Vigor2960 Series with Commtouch GlobalView Web Content Filter

SSL VPN with LDAP/RADIUS authentication

Extendability

Vigor2960 Dual WAN

IPv4/IPv6 Ready Operating System including new object-based Firewall

WAN Protocol

Ethernet	• PPPoE, PPTP, DHCP client, static IP, L2TP*, IPv6 ready

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 (Gigabit WAN) • WAN fail-over or load-balanced connectivity

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*

LDAP/Active Directory	• Lightweight directory access protocol. The enterprises use LDAP/Active Directory authentication technology to allow administrator, IT personnel and users to be authenticated when trying to access company's intranet environment.
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
GRE over IPSec	• GRE is used when IP packets need to be sent from one network to another without being parsed by any intervening routers.
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 7/Vista/XP including 32/64 bit)
Easy of Adoption	• No additional client or remote site licensing required
Industrial-standard Interoperability	• Compatible with other leading 3rd party vendor VPN devices

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 Port*	• 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'
User/Rule base	• User base integrates LDAP/Active Directory authentication to enforce policies.*

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 HTTP/TFTP/TR-069	• Using the TFTP server and the firmware upgrade utility software, you may easily upgrade to the latest firmware whenever enhanced features are added.
User Management	• Dial-in access management (PPTP/L2TP and mOTP) and LDAP/Active Directory integration.
Tag-based VLAN (802.1q)	• By means of using a VLAN ID, a tag-based VLAN can identify VLAN group membership (Support 20 VLAN groups). • Support GVRP protocol in conjunction with switch (e.g. VigorSwitch)
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 v1/v2 , MIB II
VigorACS SI Centralized Management	• TR-069 based
External Device	• Auto-detection mechanism to manage Vigor devices such as router/switch/AP
Smart Monitor Traffic Analyzer	• Support 100 PC Users

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/OSPF v2/v3*. 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.

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

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	• 4-port Gigabit switch, RJ-45
WAN	• 2-port Gigabit ethernet, RJ-45
USB	• 2 x USB host 2.0

Support

Warranty	• 2-year limited warranty, technical support through e-mail and internet FAQ/application notes
***Firmware Upgradable**	• Free firmware upgrade from Internet