DrayTek

Vigor2960 Serie

Cortafuegos de seguridad de WAN dual

- 2 puertos WAN de equilibrio de carga Gigabit Ethernet 4 puertos
- LAN Gigabit Ethernet
- 2 puertos USB para copia de seguridad 3G / 4G (o equilibrio de carga), impresora o sensor de temperatura 200 túneles
- VPN simultáneos que incluyen hasta 50 VPN SSL
- Soporte de alta disponibilidad
- Políticas flexibles de firewall, filtrado de contenido y administración de ancho de banda Administración
- central para VigorAP y VigorSwitch

La serie Vigor2960 sirve como puerta de enlace VPN y cortafuegos central para oficinas de varios sitios y teletrabajadores. Con su alto rendimiento de datos de dos Gigabit Ethernet, Dual WAN, VPN trunking y 4 puertos LAN Gigabit Ethernet, el dispositivo facilita la productividad de las operaciones comerciales versátiles. Para asegurar las comunicaciones entre sitios es el establecimiento de túneles VPN de hasta 200

túneles simultáneos.

Seguridad sin compromiso

La serie Vigor2960 también proporciona opciones de firewall de alta seguridad con protección basada en contenido y capa IP. La prevención DoS / DDoS y el filtro de contenido URL / Web refuerzan la seguridad fuera y dentro de la red. El CSM (Content Security Management) de nivel empresarial permite a los usuarios controlar y administrar las aplicaciones de mensajería instantánea (Instant Messenger) y P2P (Peer to Peer) de manera más eficiente.

Red VPN de nivel empresarial

Con un coprocesador VPN dedicado, el cifrado de hardware de AES / DES / 3DES y el hash de clave de hardware de SHA-1 / MD5 son
manejado sin problemas, manteniendo así el máximo rendimiento del enrutador. Para teletrabajadores remotos y enlaces entre oficinas, el Vigor2960 admite hasta 200 túneles VPN simultáneos (como los protocolos IPSec / PPTP / L2TP).

Sistema de gestión central

La serie Vigor2960 puede ser administrada de forma centralizada por VigorACS SI para reducir la carga de trabajo del departamento de TI. El VigorACS SI administra de manera centralizada las características esenciales del enrutador, como LAN, WAN, WLAN o VoIP sin las visitas del técnico, lo que mejora la experiencia del usuario y contribuye a costos significativos. ahorro. Por ejemplo, el administrador puede programar actualizaciones de firmware o configuración para dispositivos seleccionados al mismo tiempo. También ofrece la alerta en tiempo real para notificar al administrador cuando algo va mal, como desconexión o caída de VPN por correo electrónico y SMS para garantizar una respuesta más rápida.

Más beneficios

DrayTek ha implementado IPv6 en Vigor2960 para garantizar una ruta de migración sin problemas para la banda ancha asequible pero más rápida. La conexión WAN-IPv6 se puede establecer a través de IPv6 estático, DHCPv6 y TSPC. Hay dos puertos USB en Vigor2960. Además de la función de servidor de impresora USB, puede conectar un dispositivo móvil USB 3.5G compatible para acceder a la red celular. También puede agregar memoria de almacenamiento al puerto USB de Vigor2960 en forma de una llave de memoria USB o un disco duro USB.

Protocolo WAN

Ethernet	• PPPoE, PPTP, cliente DHCP, IP estática, L2TP *, compatible con IPv6

WAN dual

Basado en políticas de salida **Equilibrio de carga**	• Permita que su red local acceda a Internet utilizando múltiples conexiones a Internet con un alto nivel de disponibilidad de conectividad a Internet • Dos puertos WAN Ethernet dedicados (Gigabit WAN) WAN conmutación por • error o conectividad con equilibrio de carga

VPN

Protocolos	• PPTP, IPSec, L2TP, L2TP sobre IPSec
Hasta 200 sesiones simultáneamente	• LAN a LAN, acceso remoto (teletrabajador a LAN), equilibrio de carga de VPN de marcación entrante o
Troncalización de VPN	• saliente y respaldo de VPN *
LDAP / Active Directory	• Protocolo ligero de acceso a directorios. Las empresas utilizan la tecnología de autenticación LDAP / Active Directory para permitir que el administrador, el personal de TI y los usuarios se autentiquen cuando intentan acceder al entorno de intranet de la empresa.
NAT-transversal (NAT-T)	• VPN sobre rutas sin transferencia de VPN Firma
Certificado PKI	• digital (X.509)
Autenticación IKE	• Clave previamente compartida; IKE fase 1 modos agresivos / estándar y vida útil seleccionable fase 2 MD5, SHA-1 basado en
Autenticación	• hardware
Cifrado	• MPPE y AES / DES / 3DES basados en hardware
Cliente RADIUS	• Autenticación para el acceso telefónico remoto PPTP
DHCP sobre IPSec	• Debido a que DrayTek agrega una NIC virtual en la PC, por lo tanto, mientras se conecta al servidor a través del túnel IPSec, la PC obtendrá una dirección IP desde el lado remoto a través del protocolo DHCP, que es bastante similar con PPTP. GRE se usa cuando se necesitan paquetes
GRE sobre IPSec	• IP. enviado de una red a otra sin ser analizado por ningún enrutador intermedio.
Detección de pares muertos (DPD)	• Cuando hay tráfico entre los pares, no es necesario que un par envíe un mensaje de mantenimiento de vida para verificar la actividad del par porque el tráfico IPSec sirve como prueba implícita de la disponibilidad del par. Se proporciona de forma gratuita para la comodidad del
Utilidad de software Smart VPN	• teletrabajador (Windows 7 / Vista / XP, incluidos 32/64 bits)
Fácil de adopción	• No se requieren licencias adicionales de cliente o sitio remoto Compatible con otros
Interoperabilidad estándar industrial	• dispositivos VPN de terceros proveedores líderes

Funciones de enrutamiento

Enrutador	• Enrutador multiprotocolo IP y NetBIOS / IP
Enrutamiento y reenvío avanzados	• Gestión y configuración independientes completas de redes IP en el dispositivo, es decir, configuraciones individuales para DHCP, DNS, firewall, VLAN, enrutamiento, QoS, etc.
DNS	• Caché / proxy DNS
DHCP	• Cliente / relé / servidor DHCP
NTP	• Cliente NTP, ajuste automático para el horario de verano
Enrutamiento basado en políticas	• Según las reglas del firewall, ciertos tipos de datos se marcan para un enrutamiento específico, por ejemplo, a sitios o líneas remotas particulares.
Enrutamiento dinámico	• Es con el protocolo de enrutamiento de RIP v2 / OSPF v2 / v3 *. Rutas de aprendizaje y propagación; configuraciones separadas para WAN y LAN.
enrutamiento estatico	• Una instrucción para redirigir un tráfico particular a través de otra puerta de enlace local, en lugar de enviarlo a Internet con el resto del tráfico. Una ruta estática es como una "señal de desvío" en una carretera.

Filtro de contenido

Bloqueo de palabras clave de URL	• Lista blanca y lista negra • Applet de Java, cookies, Active X, comprimido, ejecutable, bloqueo de archivos multimedia Base de datos de filtrado
Filtro de contenido web	• dinámico de URL
Control de horario	• Establezca una regla de acuerdo con sus horarios de oficina específicos

Gestión del sistema

Interfaz de usuario basada en web (HTTP / HTTPS)	• Servidor web integrado para la configuración de enrutadores a través de navegadores de Internet con HTTP o HTTPS
Administración de usuarios del asistente de inicio rápido de DrayTek	• Deje que el administrador ajuste la zona horaria y configure rápidamente Internet (PPPoE, PPTP, IP estática, DHCP). Administración de usuarios • RADIUS para acceso telefónico (PPP / PPTP y ISDN CLIP).
CLI (interfaz de línea de comandos, Telnet / SSH)	• Administrar ordenadores de forma remota a través de telnet
Cliente / retransmisión / servidor DHCP	• Proporciona una función fácil de configurar para su red IP local.
DNS Dinámico	• Cuando se conecta a su ISP, por banda ancha o ISDN, normalmente se le asigna una dirección IP dinámica. es decir, la dirección IP pública asignada a su enrutador cambia cada vez que se conecta al ISP. Si desea ejecutar un servidor local, los usuarios remotos no pueden predecir su dirección IP actual para encontrarlo. La contraseña se puede aplicar a la autenticación de administradores.
Control de acceso de administración	•
Copia de seguridad / restauración de la configuración	• Si el hardware se avería, puede recuperar el sistema fallido en un tiempo aceptable. A través de TFTP, la forma efectiva es realizar una copia de seguridad y restaurar la configuración entre hosts remotos.
VLAN basada en puerto	• Cree grupos separados de usuarios segmentando cada uno de los puertos Ethernet. Por lo tanto, pueden o no comunicarse con usuarios de otros segmentos, según sea necesario.
Función de diagnóstico incorporada	• Disparador de marcación, tabla de enrutamiento, tabla de caché ARP, tabla DHCP, tabla de sesiones NAT, tabla de estaciones en línea de VLAN inalámbrica, monitor de flujo de datos, gráfico de tráfico, diagnóstico de ping, ruta de seguimiento
Cliente NTP / Programación de llamadas	• El Vigor tiene un reloj de tiempo real que puede actualizarse desde su navegador manualmente o más convenientemente automáticamente desde un servidor de tiempo de Internet (NTP). Esto le permite programar el enrutador para llamar a Internet a una hora preestablecida o restringir el acceso a Internet a determinadas horas. También se puede aplicar una programación a los perfiles de LAN a LAN (VPN o marcación directa) o algunas de las opciones de filtrado de contenido. Con el servidor TFTP y el software de utilidad de actualización de firmware, puede actualizar fácilmente al firmware más
Actualización de firmware a través de HTTP / TFTP / TR-069	• reciente siempre que se agreguen funciones mejoradas.
Gestión de usuarios	• Gestión de acceso telefónico (PPTP / L2TP y mOTP) e integración LDAP / Active Directory. Mediante el uso de una ID de VLAN, una
VLAN basada en etiquetas (802.1q)	• VLAN basada en etiquetas puede identificar la pertenencia a un grupo de VLAN (admite 20 grupos de VLAN). • Admite el protocolo GVRP junto con el interruptor (por ejemplo, VigorSwitch)
Mantenimiento Remoto	• Con Telnet / SSL, SSH (con contraseña o clave pública), navegador (HTTP / HTTPS), TFTP o SNMP, actualización de firmware a través de HTTP / HTTPS o TFTP.
Activación de la LAN	• Una PC en LAN se puede reactivar desde un estado inactivo / en espera por el enrutador que se conecta cuando recibe un paquete especial de 'activación' en su interfaz Ethernet.
Syslog	• Syslog es un método para registrar la actividad del enrutador. Gestión
Gestión SNMP	• SNMP a través de SNMP v1 / v2, basado en MIB II TR-069
Dispositivo externo de gestión centralizada	•
VigorACS SI	• Mecanismo de detección automática para administrar dispositivos Vigor como enrutador / conmutador / AP Admite 100 usuarios
Analizador de tráfico de monitor inteligente	• de PC

Gestión de ancho de banda

Modelado de tráfico	• Gestión dinámica del ancho de banda con modelado del tráfico IP
Reserva de ancho de banda	• Reserve anchos de banda mínimos y máximos por conexión basada en datos totales a través de direcciones de envío / recepción
Clasificación de puntos de código DiffServ	• Cola de prioridad de paquetes basada en DiffServ Priorización
4 niveles de prioridad (entrante / saliente)	• en términos de uso de Internet
Sesión / ancho de banda IP individual Limitación	• Definir la limitación de la sesión / ancho de banda según la dirección IP
Préstamo de ancho de banda	• Control de las velocidades de transmisión de los servicios de datos mediante el programador de paquetes Más
Reglas basadas en clases definidas por el usuario	• flexibilidad

Cortafuegos

Gestión de seguridad de contenido (CSM) Stateful	• Inspección de tráfico saliente / entrante basada en información de conexión Seguridad de puerta de enlace
Packet Inspection (SPI)	• basada en dispositivos y filtrado de contenido
Multi-NAT	• Su ISP le ha asignado varias direcciones IP públicas. Por lo tanto, puede tener una relación de uno a uno entre una dirección IP pública y una dirección IP interna / privada. Esto significa que tiene la protección de NAT (ver antes) pero la PC puede ser direccionada directamente desde el mundo exterior por su dirección IP pública con alias, pero aún abriéndole puertos específicos (por ejemplo, el puerto TCP 80 para un http / Servidor web).
Redirección de puerto	• El paquete se reenvía a una PC local específica si el número de puerto coincide con el número de puerto definido. También puede traducir el puerto externo a otro puerto localmente.
Puertos abiertos	• Como redirección de puertos (arriba) pero le permite definir un rango de puertos.
Puerto DMZ *	• Esto abre una sola PC por completo. Todos los paquetes entrantes se reenviarán al PC con la dirección IP local que configuró. Las únicas excepciones son los paquetes recibidos en respuesta a solicitudes salientes de otras PC locales o paquetes entrantes que coinciden con las reglas de los otros dos métodos. La precedencia es la siguiente: Redirección de puertos> Puertos abiertos> DMZ
Filtro de paquetes IP basado en políticas	• La información del encabezado de un paquete IP (direcciones de origen / destino IP o MAC; puertos de origen / destino; atributo DiffServ; dependiente de la dirección, dependiente del ancho de banda, dependiente del sitio remoto
Prevención DoS / DDoS	• Acto de evitar que los clientes, usuarios, clientes u otras computadoras accedan a los datos en una computadora. Comprobación de la dirección IP de
Anti-spoofing de dirección IP	• origen en todas las interfaces: solo se permiten direcciones IP clasificadas dentro de las redes IP definidas.
Cortafuegos basado en objetos	• Utiliza un enfoque orientado a objetos para la política de firewall Alerta por
Notificación	• correo electrónico y registro a través de syslog
Vincular IP a la base de reglas / usuario	• DHCP flexible con 'enlace IP-MAC'
de la dirección MAC	• La base de usuarios integra la autenticación LDAP / Active Directory para hacer cumplir las políticas. *

Internet CSM (Gestión de seguridad de contenido)

- Filtrado de palabras clave de URL: sitios específicos o palabras clave en la lista blanca o negra en las URL Bloquear
- sitios web por categoría (sujeto a suscripción)
- Impedir el acceso a sitios web mediante el uso de su dirección IP directa (por lo tanto, solo URL) Bloqueo de la
- descarga automática de subprogramas Java y controles ActiveX Bloqueo de cookies del sitio web
-
- Bloquear descargas http de tipos de archivos (binarios, comprimidos, multimedia) Horarios y exclusiones para
- habilitar / deshabilitar estas restricciones Bloquear programas de intercambio de archivos P2P (Peer-to-Peer) (por
- ejemplo, Kazaa, WinMX, etc.) Bloquear programas de mensajería instantánea (por ejemplo, IRC , MSN / Yahoo
- Messenger)

Hardware

LAN	• Switch Gigabit de 4 puertos, RJ-45 Ethernet
PÁLIDO	• Gigabit de 2 puertos, RJ-45 2 x USB host 2.0
USB	•
Fuente de alimentación	• 100-240 V, 50/60 Hz, 1,0 A