TECHNICAL SPECIFICATION

Anti-Virus

- Scan SMTP, POP3, HTTP, IMAP, FTP
- Scan ZIP/GZIP/BZIP2
- Scan encrypted VPN tunnels
- Automatic virus signature update
- Automatic alert when signature update service expires
- Real-time e-mail/syslog alert when virus is detected

Anti-Intrusion

- Rule-based detection list
- Pass/block/reset when intrusion is detected
- Automatic intrusion signature update
- Automatic alert when signature update service expires
- Real-time e-mail/syslog alert when under attack

Dual-WAN

- Outbound Policy-Based Load-Balance
- BoD (Bandwidth on Demand)
- WAN Connection Fail-over

WAN Protocol

- DHCP Client
- Static IP
- PPPoE
- PPTP
- L2TP*
- BPA

Firewall

- SPI (Stateful Packet Inspection)
- CSM (Content Security Management) for IM/ P2P Application
- Multi-NAT, DMZ Host, Port Redirection and Open Port
- Policy-Based IP Packet Filter
- DoS/DDoS Prevention
- IP Address Anti-Spoofing
- E-Mail Alert and Logging via Syslog
- Bind IP to MAC Address

Network Features

- DHCP Client/Relay/Server
- Dynamic DNS
- NTP Client
- Call Scheduling
- RADIUS Client
- DNS Cache/Proxy
- UPnP
- Port-Based VLAN
- Routing Protocol:
  - Static Routing
  - RIP V2

Content Filter

- URL Keyword Blocking (White List and Black List)
- Java Applet, Cookies, Active X, Compressed, Executable, Multimedia File Blocking
- Web Content Filter (SurfControl)
- Time Schedule Control

VPN

- Up to 200 VPN Tunnels
- Protocol : PPTP, IPSec, L2TP, L2TP over IPSec
- Encryption : MPPE and Hardware-Based AES/DES/3DES
- Authentication : Hardware-Based MD5, SHA-1
- IKE Authentication : Pre-shared Key and Digital Signature (X.509)
- LAN-to-LAN, Teleworker-to-LAN
- DHCP over IPSec
- NAT-Traversal (NAT-T)
- Dead Peer Detection (DPD)
- VPN Pass-Through

Network Management

- Web-Based User Interface (HTTP/HTTPS)
- Quick Start Wizard
- CLI (Command Line Interface, Telnet/SSH*)
- Administration Access Control
- Configuration Backup/Restore
- Built-in Diagnostic Function
- Firmware Upgrade via TFTP/FTP
- Logging via Syslog
- SNMP Management with MIB-II

Bandwidth Management

- Class-based Bandwidth Guarantee by User-Defined Traffic Categories
- DiffServ Code Point Classifying
- 4-level Priority for Each Direction (Inbound/Outbound)
- Bandwidth Borrowed
- Bandwidth/Session Limitation

Wireless Access Point (for G model)

- IEEE802.11b/g Compliant
- Super G™ 108Mbps
- Wireless Client List
- Access Point Discovery
- WDS (Wireless Distribution System)
- Wireless LAN Isolation
- Wireless Rate Control
- 64/128-bit WEP
- WPA/WPA2
- 802.1X Authentication with RADIUS Client
- Hidden SSID
- MAC Address Access Control
- Wireless VLAN

ISDN (for i model)

- Euro ISDN Compatible
- Automatic ISDN Backup
- Support 64/128Kbps (Multilink-PPP)/ BoD (Bandwidth on Demand)
- Remote Dial-In/LAN-to-LAN Connection
- Remote Activation
- Virtual TA

* Firmware Upgradeable

DrayTek

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

V1.0
991-9550000-00

CE FC

VIGORPRO 5500

UNIFIED SECURITY FIREWALL

- **All-in-one Unified Security Firewall**
  - Unified Anti-virus & Anti-intrusion threat management system
  - VPN firewall
- **Hardware-accelerated, Real-time Response**
- **Network-level Protection**
  - Block viruses at the point of network entry
  - Provide protection of all hosts inside network edge before threats intrude
- **Content-based Inline Inspection**
  - MSSI (Multi-Stack Stateful Inspection) provides deep content inline scanning
  - Scan all major network protocols
- **Less TCO (Total Cost of Ownership)**

D-SWAT

The abbreviation of "DrayTek Security Warning and Anti-attack Team".
Via its portal website, D-SWAT provides expertise with:

- **Research**
  Security information gathering and analysis
- **Training**
  Hacking techniques and incident handling
- **Service**
  Signature upgrade, news letters and on-line advisories

For more information please visit: http://www.vigorpro.com

DrayTek

Why VigorPro 5500?

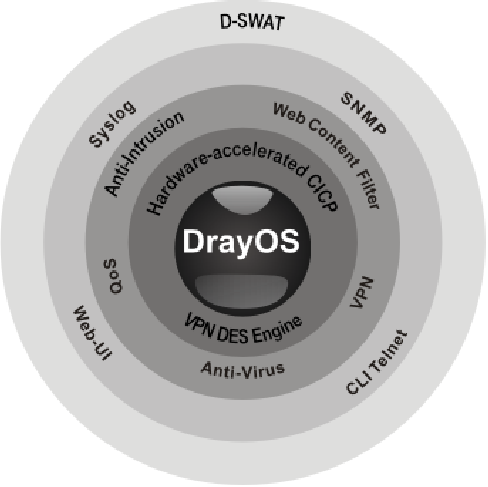
Legacy firewall devices have their limitations on networking protection and are often dedicated. The vulnerabilities of contemporary networks ranging from Web surfing, e-mail, FTP, to various instant messaging and P2P softwares, present a heavy burden for network administrators.

VigorPro5500, serving as UTM equipment of the new generation, can fulfill your requirements for secure networks.

All-in-one Unified Security Firewall

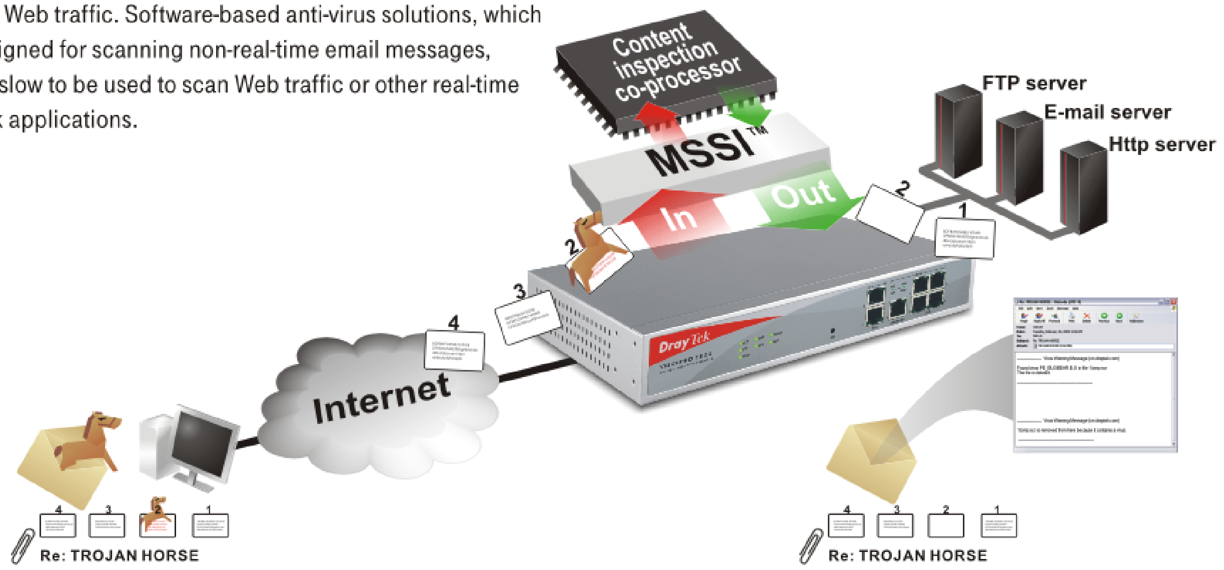
Conventional firewalls are blind to today's attacks, and also cannot detect inappropriate e-mail and Web content. The most common solution is a complex, costly collection of independent systems to deal with each of these threats along with network-level intrusions and attacks. The VigorPro 5500 is capable of providing a complete complement of integrated services including:

- Anti-virus
- Intrusion prevention
- Intrusion detection
- Web Content filter (power by SurfControl)
- VPN
- SPI Firewall



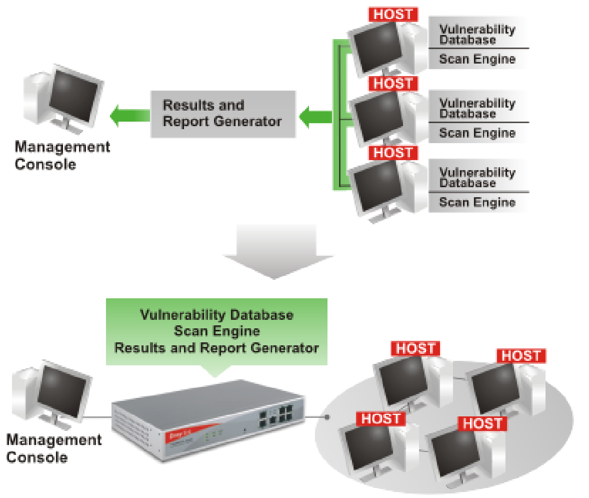
Hardware-accelerated, Real -time Response

The VigorPro 5500 employs a unique, hardware-accelerated architecture that provides the ability to perform real-time security without slowing down critical network applications, such as Web traffic. Software-based anti-virus solutions, which are designed for scanning non-real-time email messages, are too slow to be used to scan Web traffic or other real-time network applications.



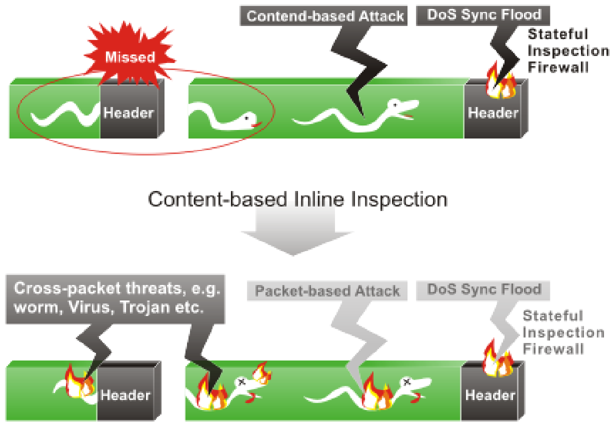
Network-level Protection

Conventional way to protect against virus or malicious program, requires each host to install software on the host. To install software on a large number of hosts is a time consuming process. To evaluate the vulnerabilities, both scan engine and database of virus pattern need constant upgrade. It is very costly and annoying for IT personnel with high maintenance. While VigorPro 5500 works as firewall as well as internet gateway, so by nature VigorPro 5500 blocks any attacks at the point of network entry. Through the web user interface, the network administrator can monitor and instruct the VigorPro 5500 to look for any vulnerability per network-level. Provide protection of all hosts inside network edge before threats intrude.



Content-based Inline Inspection

Conventional firewalls only inspect packets header to against any connection-based attack. While the content-based threats today, such as virus, worms, Trojans or banned content, spread faster and do more damage. Conventional firewalls bypass the widely spread content-based threat and expose internal network to outside world. VigorPro 5500 deploys DrayTek's unique MSSI™ (Multi-Stack Stateful Inspection) mechanism. With MSSI™,VigorPro 5500 inspects packet streams, compares any suspected content or behavior with build-in database in real-time, and provides inline anti-virus and anti-intrusion protection.


Contend-based Attack
DoS Sync Flood
Stateful Inspection Firewall
Missed
Header
Header
Content-based Inline Inspection
Cross-packet threats, e.g. worm, Virus, Trojan etc.
Packet-based Attack
DoS Sync Flood
Stateful Inspection Firewall
Header
Header

Synergy with Kaspersky Lab

VigorPro 5500 enables its anti-virus functionality by deploying Kaspersky Lab's anti-virus signature. Kaspersky Lab (http://www.kaspersky.com/) is well known as its developing and producing complete information security solutions. With over a decade of experience in the anti-virus field, Kaspersky Lab is very active in IT security associations such as CARO (Computer Antivirus Research Organization) and ICSA (International Computer Security Association). That's why Kaspersky Lab is able to predict data security trends and react to up to the minute IT security threat. With the synergy of DrayTek and Kaspersky Lab, VigorPro 5500 provides enterprise with the best protection against network threat.

KASPERSKY ANTI•VIRUS

DrayTek