FEATURES

Unified Threat Management

+ Check Point® Stateful Inspection Firewall
+ Hardware-based VPN Firewall
+ Gateway Antivirus
+ Integrated Secure Wireless Connectivity (DFL-CPG310 Only)

Secure Remote User Access

+ VPN-1® SecuRemote™ Licenses Included
+ User Limit Upgradeable

Traffic Shaper (QoS)

+ Predefined Classes
+ Ideal for VoIP or Videoconferencing

Versatile Management

+ Wizard Driven Web UI
+ Secure HTTP
+ CLI (SSH & Serial COM)

Security Service Upgrades

+ Antivirus Service
+ Content Filter Service
+ Updates Service

NetDefend™ secured by Check Point®

Firewall/VPN Security Appliances

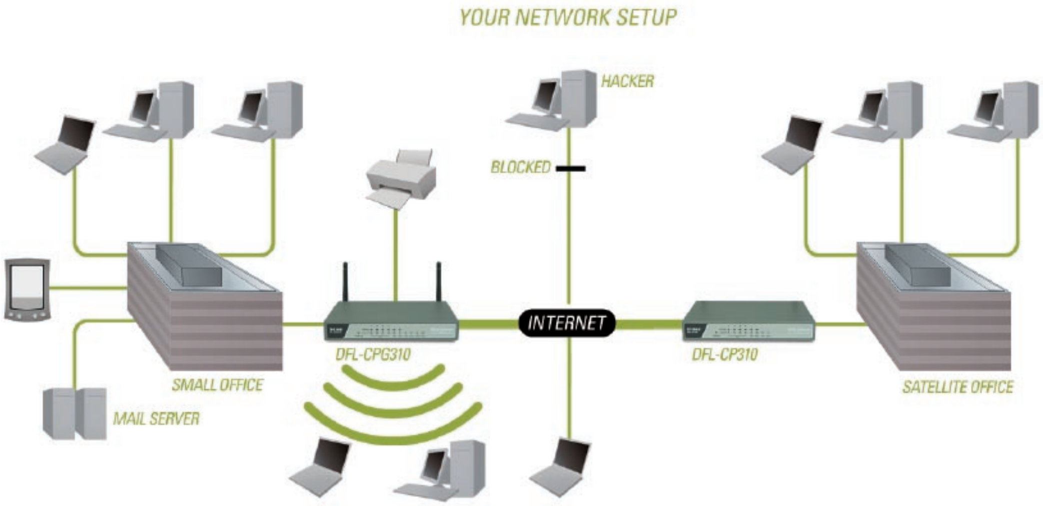
D-Link introduces the NetDefend™ secured by Check Point® line of Firewall/VPN Security Appliances. With the growing concerns over network security and increasing emphasis on protecting customer privacy, D-Link's NetDefend secured by Check Point line of security appliances provide the assurance of dedicated network security in a single device.

These security appliances deliver unified threat management for small and medium businesses that require maximum security with limited device administration. NetDefend secured by Check Point security appliances offer advanced, adaptable, all-in-one security at cost-effective prices, delivering integrated firewall, VPN, antivirus, content filtering, and upgrade services. With NetDefend handling your network security, devote more time to the business side of your business.

Proven Check Point Technology

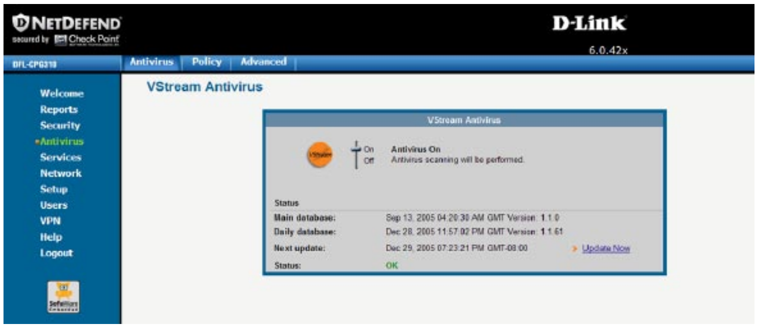
The NetDefend secured by Check Point series of hardware-based VPN firewalls are designed to deliver advanced performance and comprehensive security in a single, easy-to-deploy solution. NetDefend secured by Check Point firewalls provide complete protection using Check Point's patented Stateful Inspection technology. These single-box solutions use the same firewall technology that keeps 97% of Fortune 500 companies up and running.

Check Point's Stateful Inspection technology monitors and blocks attacks on your network. This firewall technology based on INSPECT, protects your network and all devices on it by implementing rules that allow or deny access to them. It delivers greater protection against hackers than packet filter or Network Address Translation-based firewalls by thoroughly examining and retaining information contained in data packets. These security appliances automatically determine whether communication attempts are legitimate, making your network safe from attacks.



Active Intelligence for Active Threats

These firewall appliances block viruses at the firewall, providing protection to all the PCs in your network, even if they do not have all the latest patches and updates installed. And since new threats and exploits are found daily, the firewall is the most important line of defense for your business. Using an antivirus service at the gateway allows you to have a single point of control for blocking viruses before they enter your network. The antivirus policy setup provides a simple and quick way to define which communications should be scanned. By incorporating a gateway antivirus in parallel with desktop antivirus software, you can assure protection against zero-hour virus outbreaks and provide an additional layer of protection against viruses that have yet to be created.



VStream Antivirus

VStream Antivirus

Antivirus On
Antivirus scanning will be performed.

Status

Main database:	Sep 13, 2005 04:20:30 AM GMT Version: 1.1.0
Daily database:	Dec 28, 2005 11:57:02 PM GMT Version: 1.1.61
Next update:	Dec 29, 2005 07:23:21 PM GMT-08:00
Status:	OK

Check Point Application Intelligence technology allows the NetDefend Security Appliance to block denial of service (DoS) attacks, detect protocol anomalies, limit application ability to carry malicious data and control application-layer operations. These mechanisms aid proper usage of Internet resources, such as instant messaging, Peer-to-Peer (P2P) file sharing and File Transfer Protocol (FTP), and allow you to block questionable traffic and ensure that your bandwidth is used in the most efficient and secure way possible.

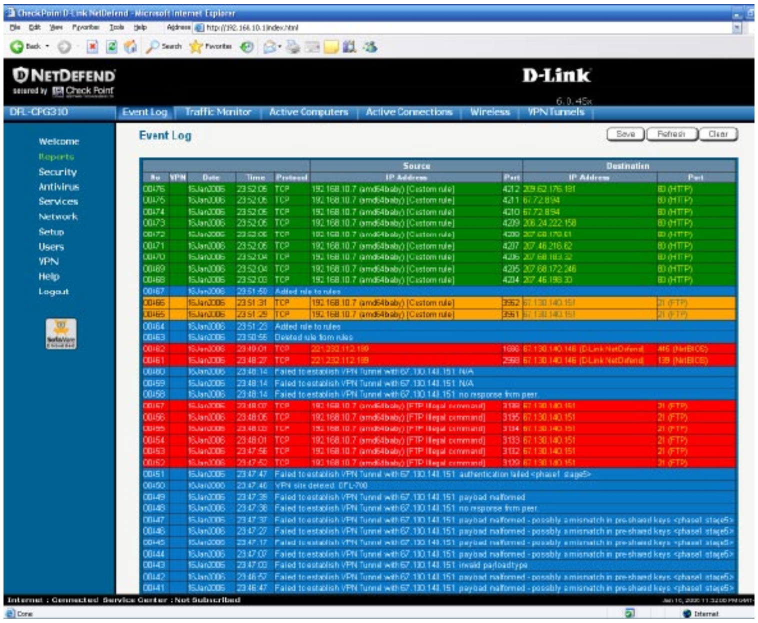
Secure Remote User Access

Road warriors and telecommuters can securely access the office network using the VPN capabilities of the NetDefend secured by Check Point series. These products offer secure remote access and management while also providing secure LAN access using the highly secure IPSec VPN protocol. The integrated IPSec VPN server not only allows secure encrypted communications from the Internet, but also allows LAN (WLAN) clients the ability to maximize network security by forming IPSec tunnels to the device. These appliances include Check Point's VPN-1® SecuRemote™ software for installation on client devices to access the network.

As your business expands and VPN usage increases, the NetDefend secured by Check Point Security Appliance has the ability to upgrade the allowed number of concurrent users. User support may be incrementally increased all the way to an unrestricted state, ensuring that these security appliances can grow with your business, providing secure remote access now and for years to come.

Designed to Improve Operating Efficiency

Keeping your network up and running is critical to your business' operating efficiency. To address this need, NetDefend secured by Check Point firewalls feature dual WAN ports for failover support. Since the Internet Service Provider (ISP) connection can sometimes be the weakest link, the dual WAN ports can be used to support a backup broadband or dial-up ISP connection (external modem required), in case of connection failures.



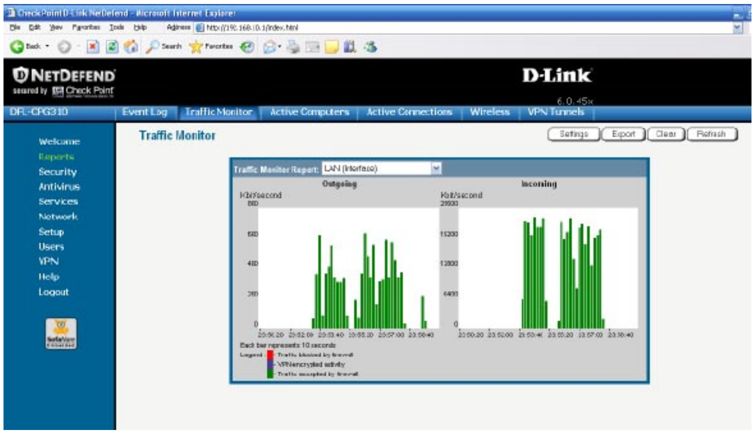
Event Log

					Source		Destination	
No	VPN	Date	Time	Protocol	IP Address	Port	IP Address	Port
00476		15Jan2006	23:52:05	TCP	192.168.10.7 (amd64baby) [Custom rule]	4212	209.62.176.181	80 (HTTP)
00475		15Jan2006	23:52:05	TCP	192.168.10.7 (amd64baby) [Custom rule]	4211	67.72.8.94	80 (HTTP)
00474		15Jan2006	23:52:05	TCP	192.168.10.7 (amd64baby) [Custom rule]	4210	67.72.8.94	80 (HTTP)
00473		15Jan2006	23:52:05	TCP	192.168.10.7 (amd64baby) [Custom rule]	4209	206.24.222.158	80 (HTTP)
00472		15Jan2006	23:52:05	TCP	192.168.10.7 (amd64baby) [Custom rule]	4208	207.68.170.61	80 (HTTP)
00471		15Jan2006	23:52:05	TCP	192.168.10.7 (amd64baby) [Custom rule]	4207	207.46.216.62	80 (HTTP)
00470		15Jan2006	23:52:04	TCP	192.168.10.7 (amd64baby) [Custom rule]	4206	207.68.183.32	80 (HTTP)
00469		15Jan2006	23:52:04	TCP	192.168.10.7 (amd64baby) [Custom rule]	4205	207.68.172.246	80 (HTTP)
00468		15Jan2006	23:52:03	TCP	192.168.10.7 (amd64baby) [Custom rule]	4204	207.46.198.30	80 (HTTP)
00467		15Jan2006	23:51:50	Added rule to rules				
00466		15Jan2006	23:51:31	TCP	192.168.10.7 (amd64baby) [Custom rule]	3952	67.130.140.151	21 (FTP)
00465		15Jan2006	23:51:29	TCP	192.168.10.7 (amd64baby) [Custom rule]	3951	67.130.140.151	21 (FTP)
00464		15Jan2006	23:51:23	Added rule to rules				
00463		15Jan2006	23:50:55	Deleted rule from rules				
00462		15Jan2006	23:49:01	TCP	221.232.112.189	1686	67.130.140.146 (D-Link NetDefend)	445 (NetBIOS)
00461		15Jan2006	23:48:27	TCP	221.232.112.189	2568	67.130.140.146 (D-Link NetDefend)	139 (NetBIOS)
00460		15Jan2006	23:48:14	Failed to establish VPN Tunnel with 67.130.140.151: N/A				
00459		15Jan2006	23:48:14	Failed to establish VPN Tunnel with 67.130.140.151: N/A				
00458		15Jan2006	23:48:14	Failed to establish VPN Tunnel with 67.130.140.151: no response from peer.				
00457		15Jan2006	23:48:07	TCP	192.168.10.7 (amd64baby) [FTP Illegal command]	3136	67.130.140.151	21 (FTP)
00456		15Jan2006	23:48:05	TCP	192.168.10.7 (amd64baby) [FTP Illegal command]	3135	67.130.140.151	21 (FTP)
00455		15Jan2006	23:48:03	TCP	192.168.10.7 (amd64baby) [FTP Illegal command]	3134	67.130.140.151	21 (FTP)
00454		15Jan2006	23:48:01	TCP	192.168.10.7 (amd64baby) [FTP Illegal command]	3133	67.130.140.151	21 (FTP)
00453		15Jan2006	23:47:56	TCP	192.168.10.7 (amd64baby) [FTP Illegal command]	3132	67.130.140.151	21 (FTP)
00452		15Jan2006	23:47:52	TCP	192.168.10.7 (amd64baby) [FTP Illegal command]	3129	67.130.140.151	21 (FTP)
00451		15Jan2006	23:47:47	Failed to establish VPN Tunnel with 67.130.140.151: authentication failed <phase1 stage5>				
00450		15Jan2006	23:47:46	VPN site deleted: DFL-700				
00449		15Jan2006	23:47:39	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed				
00448		15Jan2006	23:47:38	Failed to establish VPN Tunnel with 67.130.140.151: no response from peer.				
00447		15Jan2006	23:47:37	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed - possibly a mismatch in pre-shared keys <phase1 stage5>				
00446		15Jan2006	23:47:27	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed - possibly a mismatch in pre-shared keys <phase1 stage5>				
00445		15Jan2006	23:47:17	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed - possibly a mismatch in pre-shared keys <phase1 stage5>				
00444		15Jan2006	23:47:07	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed - possibly a mismatch in pre-shared keys <phase1 stage5>				
00443		15Jan2006	23:47:03	Failed to establish VPN Tunnel with 67.130.140.151: invalid payloadtype				
00442		15Jan2006	23:46:57	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed - possibly a mismatch in pre-shared keys <phase1 stage5>				
00441		15Jan2006	23:46:47	Failed to establish VPN Tunnel with 67.130.140.151: payload malformed - possibly a mismatch in pre-shared keys <phase1 stage5>				

Internet : Connected Service Center : Not Subscribed

Jan 16, 2006 11:32:00 PM GMT-

The NetDefend firewalls log information on attempted attacks and displays it in an easy-to-follow, color-coded report. This provides power capabilities that enable you to see the IP address from which an attack originated. A "Who Is" utility enables you to identify an IP address's owner, giving you Internet "caller ID" capability. In addition, the security Appliances provide built-in traffic monitoring and packet capture tools that provide the means for controlling and monitoring incoming and outgoing traffic to ensure efficient utilization of your broadband connection.



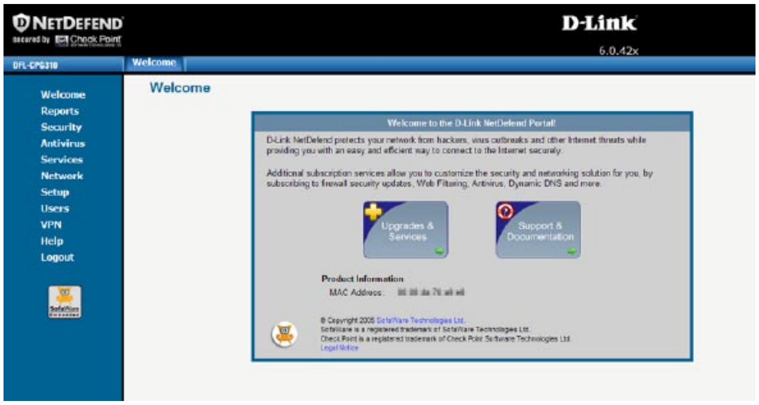
Traffic Monitor

Traffic Monitor Report: LAN (Interface)

Each bar represents 10 seconds

Customized to Suit Your Business

The NetDefend's simple web-based management enables you to secure your business in minutes. After accessing the setup wizard, you can select one of three pre-set firewall policies (high, medium, or low) or create your own custom security policy. Either way, the setup wizard quickly takes you through the steps of policy creation. Your security rules are as flexible as your business needs dictate – and you can change them at any time and from any place – using a variety of remote management options.



Welcome

Welcome to the D-Link NetDefend Portal!

D-Link NetDefend protects your network from hackers, virus outbreaks and other Internet threats while providing you with an easy and efficient way to connect to the Internet securely.

Additional subscription services allow you to customize the security and networking solution for you, by subscribing to firewall security updates, Web Filtering, Antivirus, Dynamic DNS and more.

Product Information
MAC Address: [redacted]

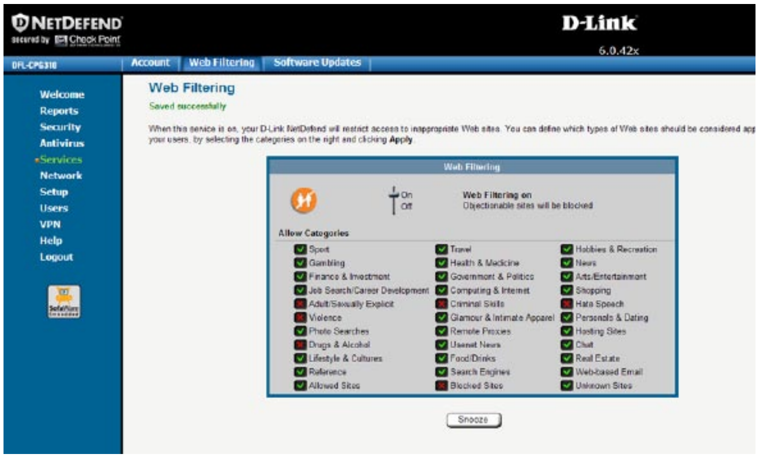
© Copyright 2005 SofaWare Technologies Ltd.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point is a registered trademark of Check Point Software Technologies Ltd.
Legal Notice

The NetDefend Security Appliance also includes Traffic Shaper, a comprehensive bandwidth management Quality of Service (QoS) system that enables the administrator to fully control the traffic flow, by assigning weighted priorities, limits, and guaranteed bandwidth for different types of traffic. Improve the quality of time-sensitive applications such as VoIP or videoconferencing.

Active Vigilance

For effective protection against new and evolving threats, your network's security solution must be kept up to date. You can update software automatically, with no user interaction required, by subscribing to the NetDefend Security Service. The service not only keeps your software and virus definitions up to date, but also generates monthly security reports that provide in-depth information on traffic, firewall activity, antivirus activity, and more. A limited-trial period is included with the purchase of a NetDefend Security Appliance .

In addition to software updates, NetDefend Security Service subscription can also enable web filtering and Dynamic DNS. Web filtering allows you to increase productivity and reduce network exposure to Internet threats by limiting access to inappropriate content. Additionally, a Dynamic DNS service provided by the NetDefend Security Service allows you to use an easy-to-remember web address for your device. Provides customers, partners, and employees access to key resources via VPN without having to know an ever-changing IP address.



Web Filtering

Saved successfully

When this service is on, your D-Link NetDefend will restrict access to inappropriate Web sites. You can define which types of Web sites should be considered app
your users, by selecting the categories on the right and clicking **Apply**.

Web Filtering

Web Filtering on
Objectionable sites will be blocked

Allow Categories

☑ Sport	☑ Travel	☑ Hobbies & Recreation
☑ Gambling	☑ Health & Medicine	☑ News
☑ Finance & Investment	☑ Government & Politics	☑ Arts/Entertainment
☑ Job Search/Career Development	☑ Computing & Internet	☑ Shopping
☒ Adult/Sexually Explicit	☒ Criminal Skills	☒ Hate Speech
☒ Violence	☑ Glamour & Intimate Apparel	☑ Personals & Dating
☑ Photo Searches	☑ Remote Proxies	☑ Hosting Sites
☒ Drugs & Alcohol	☑ Usenet News	☑ Chat
☑ Lifestyle & Cultures	☑ Food/Drinks	☑ Real Estate
☑ Reference	☑ Search Engines	☑ Web-based Email
☑ Allowed Sites	☒ Blocked Sites	☑ Unknown Sites

You can choose a variety of services and packages to add functionality to your NetDefend firewall. They range from the basic service, which includes product support, software updates, and Dynamic DNS service, all the way up to the PowerPack, which includes multiple license upgrades for VPN connections, site tunnels, VPN throughput, firewall throughput, advanced QoS, support for VLAN tagging and more. Regardless of your network demands, the NetDefend secured by Check Point line of Firewall/VPN Security Appliances can adapt to your small business needs.

Wireless and Print Server Functionality

The DFL-CPG310 model adds secure WLAN access via its built-in 802.11b/g access point, featuring D-Link 108G technology. WLAN deployments in office environments typically open up the private network to anyone possessing a wireless card and a little expertise. The DFL-CPG310 model isolates WLAN and LAN traffic to prevent unauthorized access to LAN resources through the WLAN interface. Add on top of this the latest WPA security mechanisms and the ability to run IPSec over wireless, and the DFL-CPG310 becomes very attractive to those looking to deploy a secure WLAN to augment their secure LAN. In terms of compatibility, the integrated access point can service 802.11b, 802.11g, and D-Link 108G WLAN clients with ease. The DFL-CPG310 also adds a built-in print server, enabling any USB-enabled printer to become a wireless network printer to save you the investment in a more expensive network printer or a standalone print server.

The NetDefend secured by Check Point line of Firewall/VPN Security Appliances provide VARs, ISPs, and other solution providers with the ideal product for implementation for their small business customers. For VARs and Service Providers that target small businesses, support for Security Management Portal (SMP) Servers create an innovative opportunity for device management. Once a NetDefend secured by Check Point device is configured to access a SMP Server, additional features can be unlocked to maximize the potential of these products.

The SMP integration of the NetDefend secured by Check Point firewalls enables the ability to provide advanced remote management. A single SMP can be used with an unlimited number of NetDefend Firewalls, providing a VAR, ISP or solution provider with the potential for reduced maintenance costs with fewer on-site service requests while increasing overall network efficiency.

SMP support for these devices also enables support for Dynamic VPN. Dynamic VPN enables administrators to define VPN communities and configure security parameters for the entire VPN quickly and easily. Adding VPN users is simplified, since they automatically inherit settings from the community. Dynamic VPN also tracks the IP addresses of the NetDefend firewalls and updates the address in the VPN end points.

Larger VARs and small ISPs can also take advantage of network-based spam filtering, preventing spam messages from reaching their customer's network. SMP spam filtering gives the VAR the option to use either the built-in spam filter or a third-party OPSEC CVP-based scanner.

Software

Firewall
+ 6,000 Concurrent Connections
+ Stateful Inspection Firewall
+ 3-Level Preset Security Policies
+ Firewall Customization Wizard

VPN
+ 20Mbps Performance (3DES)
+ Site-to-site IPSec VPN
+ Remote Access VPN Gateway
+ 5 VPN-1 SecuRemote Client Licenses Included
+ AES, 3DES, and DES Encryption
+ Authentication: SHA1/MD5
+ IPSec NAT Traversal
+ VPN Site Wizard

Networking
+ WAN Access Protocols:
  + Static IP
  + PPPoE
  + Telstra
  + DHCP
  + PPTP
+ Traffic Shaper (QoS) Predefined Classes
+ Static NAT
+ Hide NAT
+ PAT
+ DHCP Server
+ MAC Cloning
+ Static Routes
+ Internet Connection Setup Wizard
+ Digital Certificates (X.509)
+ Failover WAN (Ethernet or Dialup)

Logging and Monitoring
+ Advanced Attack & Audit Logs
+ Syslog Logging
+ Graphical Map of Network & VPN Tunnels
+ Packet Capture Utility

Local Management
+ Web-based Management
+ HTTPS Remote Management
+ CLI (Command Line Interface)
+ SSH Remote Management

Upgrades
+ User limit Upgradeable (10, 25, Unlimited)
+ Services Upgradeable (Web Filter, Antivirus)

Printer Server (DFL-CPG310 only)
+ 2 USB Ports

WLAN Security (DFL-CPG310 only)
+ VPN over Wi-Fi
+ WEP (64, 128-bit)
+ WPA, WPA-PSK
+ WPA2, WPA2-Personal
+ 802.1x
+ 802.11i

Physical & Environmental

Device Ports:
+ WAN: 1 10/100BASE-TX Port
+ LAN: 4 10/100BASE-TX Ports
+ DMZ/WAN2: 10/100BASE-TX Port
+ WLAN: Wi-Fi 802.11b/g/108G (DFL-CPG310 only)
+ Console Port: Serial COM Port
+ USB Port: 2 x USB 2.0 (DFL-CPG310 only)

Diagnostic LED
+ Power
+ WAN (Link/Activity per Port) (2)
+ LAN (Link/Activity per Port) (8)
+ DMZ/WAN2 (Link/Activity per Port) (2)
+ VPN
+ Serial
+ USB

Power Input
External Power Supply (5VDC, 3.0A)

Power Consumption
15 Watts Max.

Dimensions
7.875" x 5.0" x 1.25"

Weight
1.8lbs

Temperature
+ Operating: 32°F to 140°F
+ Storage: -4°F to 158°F

Humidity
5% to 95% (non-condensing)

Emission (EMI)
+ FCC Class B
+ CE Class B

Safety
+ UL
+ LVD (EN60950)

D-Link Systems, Inc. 17595 Mt Herrmann, Fountain Valley CA, 92708-4160 www.dlink.com
All references to speed are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.
Visit www.dlink.com for more details.