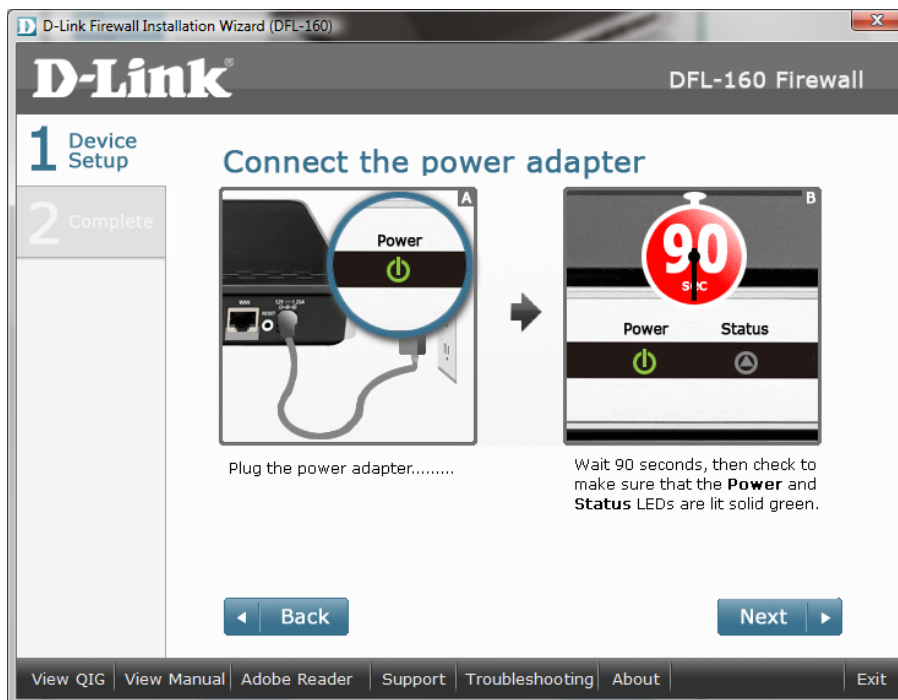


DFL-160
UTM Firewall for SOHO

CD 1.0

Firmware 2.25.01



D-Link Firewall Installation Wizard (DFL-160) D-Link Firewall

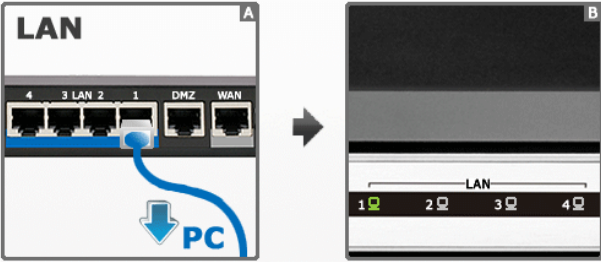
D-Link

DFL-160 Firewall

1 Device Setup

2 Complete

Connect the LAN Ethernet cable



Connect your PC's network port to one of the LAN ports on the DFL-160.

Ensure that the **LAN** LED on the front of your DFL-160 are lit solid green.

[Back](#) [Next](#)

[View QIG](#) [View Manual](#) [Adobe Reader](#) [Support](#) [Troubleshooting](#) [About](#) [Exit](#)

D-Link Firewall Installation Wizard (DFL-160) D-Link Firewall

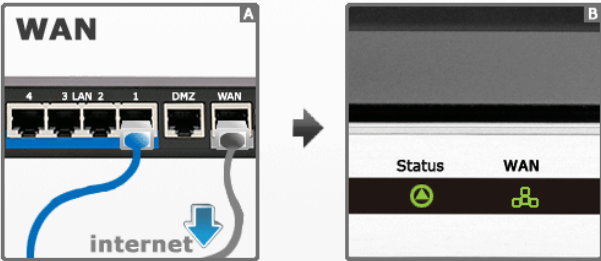
D-Link

DFL-160 Firewall

1 Device Setup

2 Complete

Connect the WAN Ethernet cable

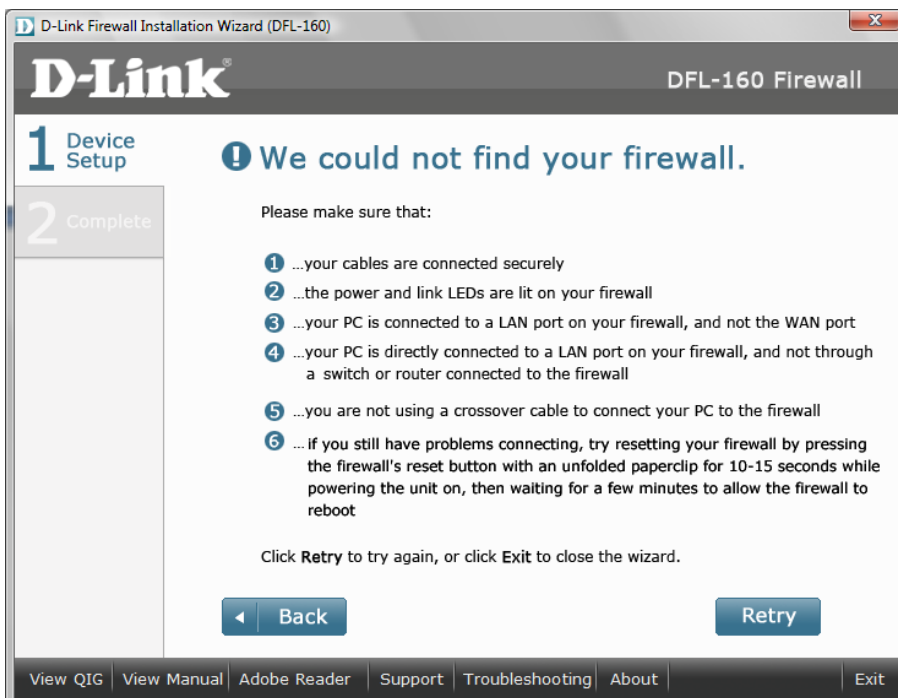
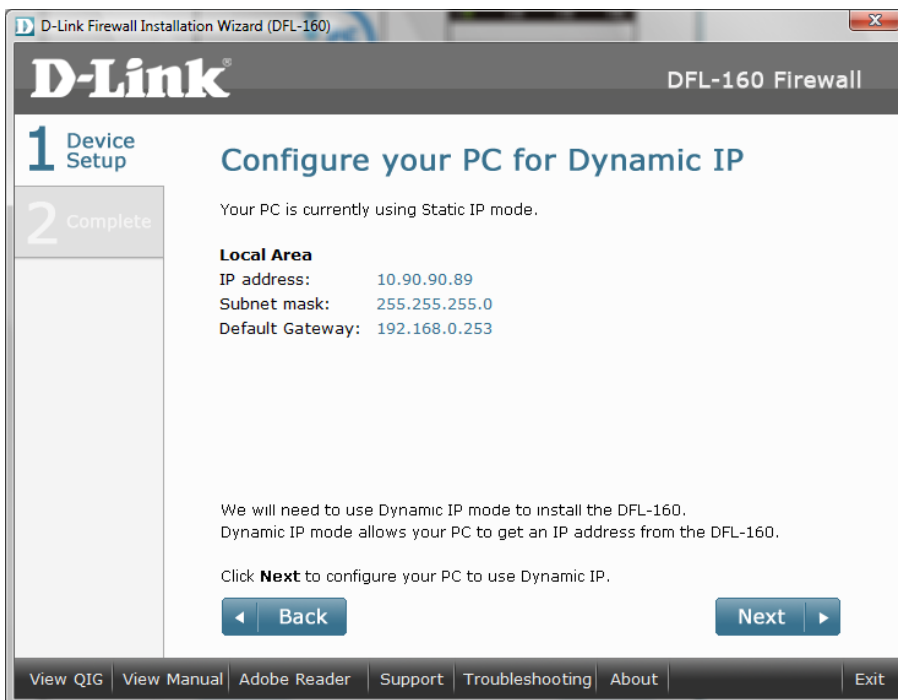


Connect your Internet cable or network device to the WAN port of the DFL-160.

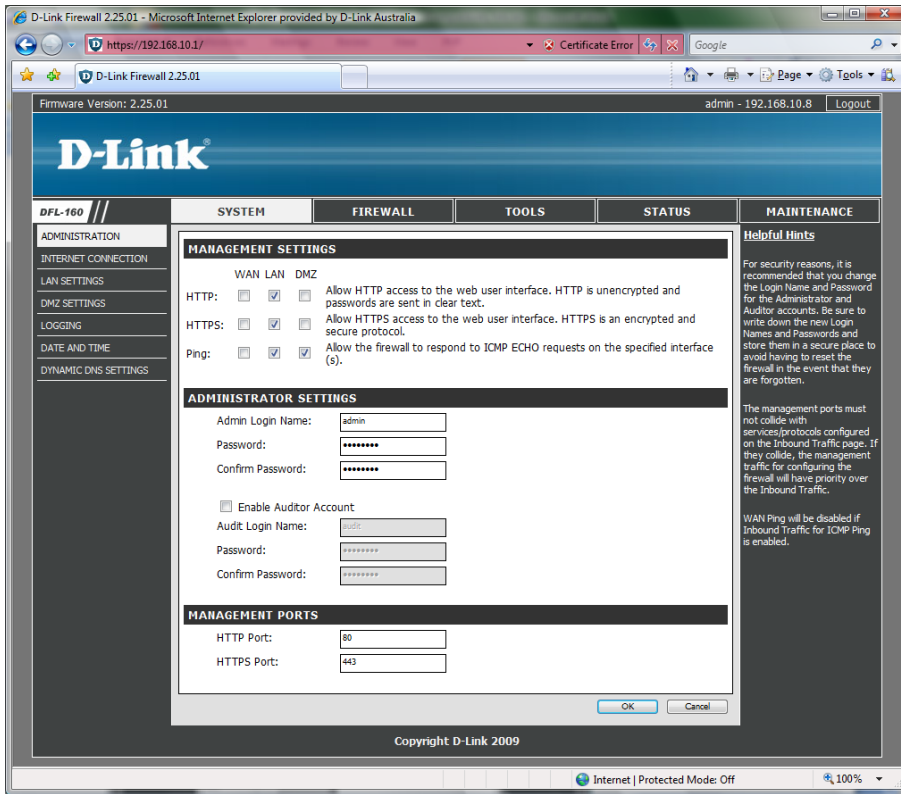
Ensure that the **WAN** LED on the front of your DFL-160 are lit solid green.

[Back](#) [Next](#)

[View QIG](#) [View Manual](#) [Adobe Reader](#) [Support](#) [Troubleshooting](#) [About](#) [Exit](#)







D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- ADMINISTRATION
- INTERNET CONNECTION
- LAN SETTINGS
- DMZ SETTINGS
- LOGGING
- DATE AND TIME
- DYNAMIC DNS SETTINGS

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

GENERAL

Configure the connection type used for accessing the Internet.

Internet Connection Type:

DHCP SETUP

When using DHCP, the device will automatically retrieve all required IP addresses from your ISP.

MTU: Should normally not be changed

STATIC CONNECTION

Static WAN interface configuration is most commonly used in dedicated-line Internet connections.

IP:

Network:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

MTU: Should normally not be changed

PPPOE CONNECTION

PPP over Ethernet connections are used in many DSL and cable modem networks. Internet connection settings are assigned automatically after authentication.

Username:

Password:

Confirm Password:

Service Name: Some ISPs require a service name

Helpful Hints

The default WAN interface setting is DHCP which will retrieve all required IP addresses automatically from a DHCP server without any further configuration changes.

When configuring other methods to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, please contact your Internet Service Provider (ISP).

If you are having trouble accessing the Internet through the firewall, double check any settings you have entered on this page and verify them with your ISP.

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- ADMINISTRATION
- INTERNET CONNECTION
- LAN SETTINGS
- DMZ SETTINGS
- LOGGING
- DATE AND TIME
- DYNAMIC DNS SETTINGS

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

Changes in the configuration have not been saved.

GENERAL

Configure the connection type used for accessing the Internet.

Internet Connection Type:

DHCP SETUP

When using DHCP, the device will automatically try to retrieve the WAN settings from your ISP.

MTU: Should normally not be changed

STATIC CONNECTION

Static WAN interface configuration is most commonly used in dedicated-line Internet connections.

IP:

Network:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

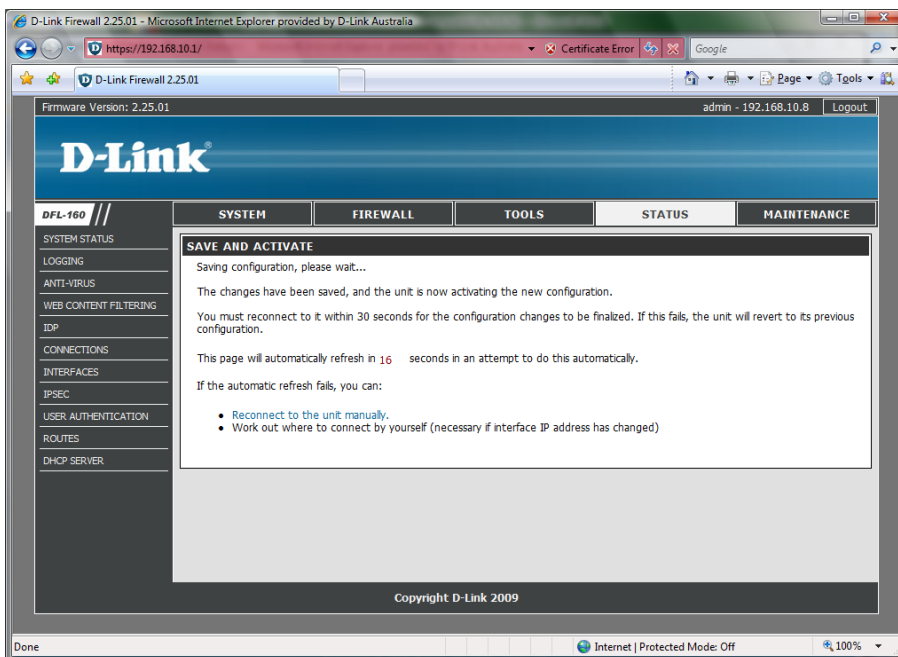
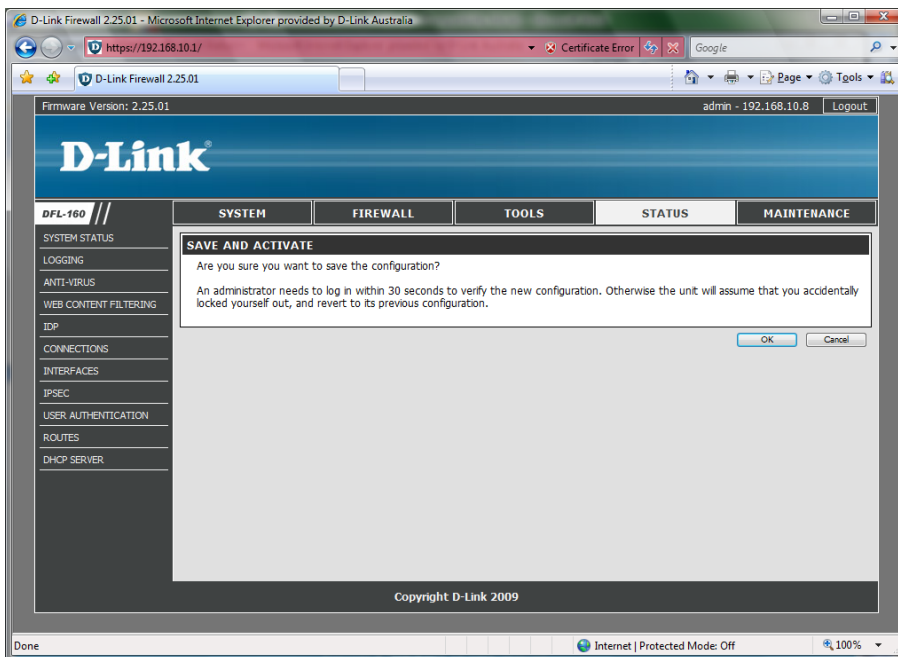
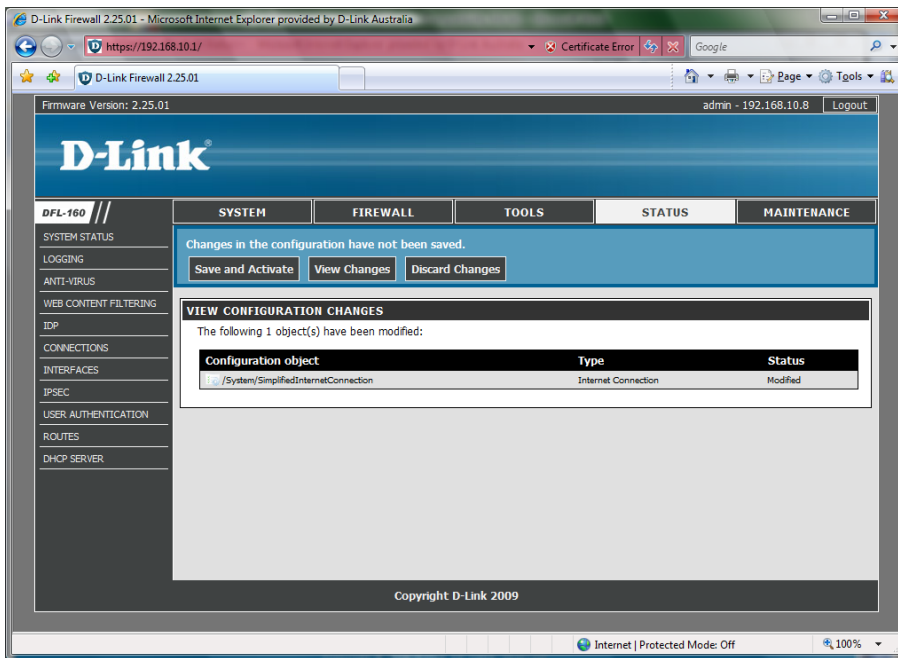
Helpful Hints

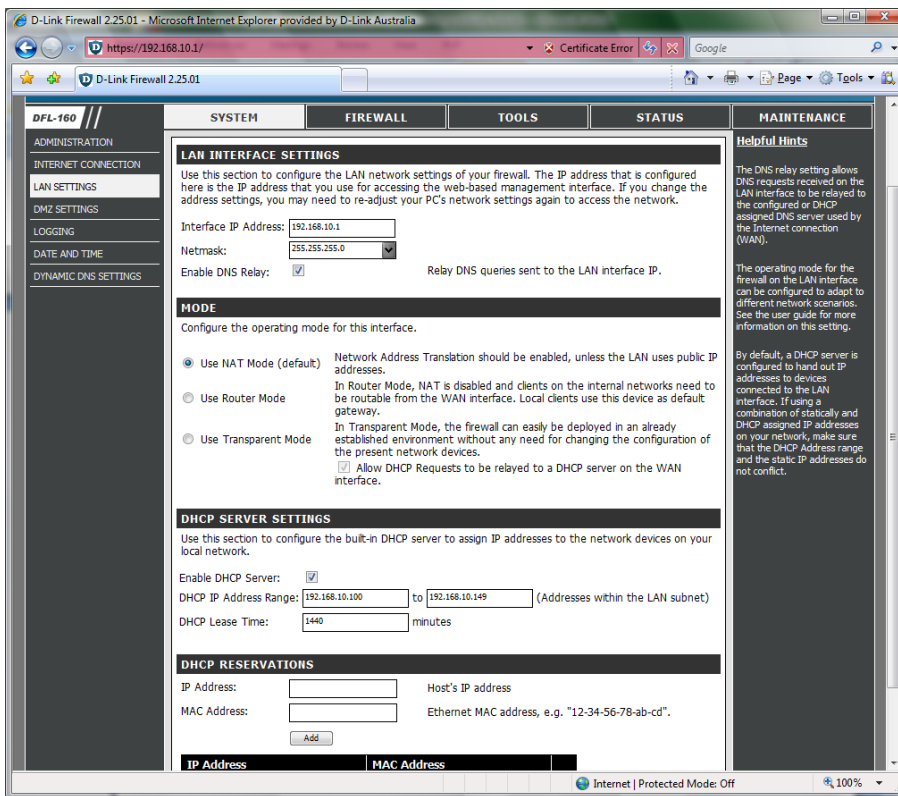
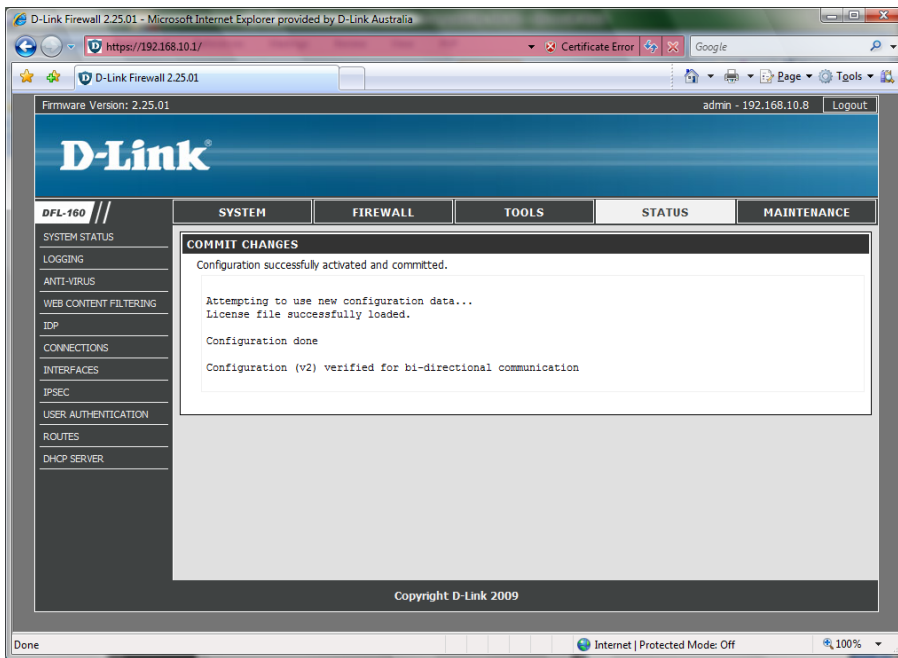
The default WAN interface setting is DHCP which will retrieve all required IP addresses automatically from a DHCP server without any further configuration changes.

When configuring other methods to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, please contact your Internet Service Provider (ISP).

If you are having trouble accessing the Internet through the firewall, double check any settings you have entered on this page and verify them with your ISP.

Internet | Protected Mode: Off 100%





D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/

D-Link Firewall 2.25.01

SYSTEM	FIREWALL	TOOLS	STATUS	MAINTENANCE				
LAN INTERFACE SETTINGS Use this section to configure the LAN network settings of your firewall. The IP address that is configured here is the IP address that you use for accessing the web-based management interface. If you change the address settings, you may need to re-adjust your PC's network settings again to access the network.								
Interface IP Address: <input type="text" value="192.168.10.1"/> Netmask: <input type="text" value="255.255.255.0"/>								
Enable DNS Relay: <input type="checkbox"/> Relay DNS queries sent to the LAN interface IP.								
MODE Configure the operating mode for this interface.								
<input checked="" type="radio"/> Use NAT Mode (default) Network Address Translation should be enabled, unless the LAN uses public IP addresses.								
<input type="radio"/> Use Router Mode In Router Mode, NAT is disabled and clients on the internal networks need to be routable from the WAN interface. Local clients use this device as default gateway.								
<input type="radio"/> Use Transparent Mode In Transparent Mode, the firewall can easily be deployed in an already established environment without any need for changing the configuration of the present network devices.								
<input type="checkbox"/> Allow DHCP Requests to be relayed to a DHCP server on the WAN interface.								
DHCP SERVER SETTINGS Use this section to configure the built-in DHCP server to assign IP addresses to the network devices on your local network.								
Enable DHCP Server: <input checked="" type="checkbox"/>								
DHCP IP Address Range: <input type="text" value="192.168.10.100"/> to <input type="text" value="192.168.10.149"/> (Addresses within the LAN subnet)								
DHCP Lease Time: <input type="text" value="1440"/> minutes								
DHCP RESERVATIONS								
IP Address: <input type="text"/> Host's IP address								
MAC Address: <input type="text"/> Ethernet MAC address, e.g. "12-34-56-78-ab-cd".								
<input type="button" value="Add"/>								
<table border="1"> <thead> <tr> <th>IP Address</th> <th>MAC Address</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>					IP Address	MAC Address		
IP Address	MAC Address							

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/

D-Link Firewall 2.25.01

SYSTEM	FIREWALL	TOOLS	STATUS	MAINTENANCE
DMZ INTERFACE SETTINGS Use this section to configure the DMZ network settings of your firewall. The IP address that is configured here is the IP address that you use for accessing the web-based management interface. If you change the address settings, you may need to re-adjust your PC's network settings again to access the network.				
Interface IP Address: <input type="text" value="192.168.11.1"/> Netmask: <input type="text" value="255.255.255.0"/>				
Enable DNS Relay: <input checked="" type="checkbox"/> Relay DNS queries sent to the DMZ interface IP.				
MODE Configure the operating mode for this interface.				
<input checked="" type="radio"/> Use NAT Mode (default) Network Address Translation should be enabled, unless the DMZ uses public IP addresses.				
<input type="radio"/> Use Router Mode In Router Mode, NAT is disabled and clients on the internal networks need to be routable from the WAN interface. Local clients use this device as default gateway.				
<input type="radio"/> Use Transparent Mode In Transparent Mode, the firewall can easily be deployed in an already established environment without any need for changing the configuration of the present network devices.				
<input type="checkbox"/> Allow DHCP Requests to be relayed to a DHCP server on the WAN interface.				
DHCP SERVER SETTINGS Use this section to configure the built-in DHCP server to assign IP addresses to the network devices on your local network.				
Enable DHCP Server: <input checked="" type="checkbox"/>				
DHCP IP Address Range: <input type="text" value="192.168.11.100"/> to <input type="text" value="192.168.11.149"/> (Addresses within the DMZ subnet)				
DHCP Lease Time: <input type="text" value="1440"/> minutes				
DHCP RESERVATIONS				
IP Address: <input type="text"/> Host's IP address				
MAC Address: <input type="text"/> Ethernet MAC address, e.g. "12-34-56-78-ab-cd".				
<input type="button" value="Add"/>				

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

ADMINISTRATION

INTERNET CONNECTION

LAN SETTINGS

DMZ SETTINGS

LOGGING

DATE AND TIME

DYNAMIC DNS SETTINGS

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

SYLOG SETTINGS

Send log data via the syslog protocol to one or two syslog servers

Syslog Server 1:

Syslog Server 2: (optional)

Syslog Facility:

AUDIT LOGGING

The firewall normally logs denied packets. With audit logging enabled, it will also log when allowed connections are opened and closed.

Enable Audit Logging

EMAIL ALERTING

Enable Email Alerting for IDP (Intrusion Detection & Prevention) events.

Sensitivity: Specifies the sensitivity level for sending IDP log events

SMTP Server IP: SMTP server for logs

Sender Name:

Email Address 1:

Email Address 2:

Email Address 3: (optional)

OK Cancel

Copyright D-Link 2009

Helpful Hints

The internal logger has limited storage and will not preserve logs after a restart of the firewall. Firewall logs can be sent to external Syslog servers for backup and storage as well as analysis.

The Intrusion Detection and Prevention system can send log message alerts to a configured SMTP server IP.

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

ADMINISTRATION

INTERNET CONNECTION

LAN SETTINGS

DMZ SETTINGS

LOGGING

DATE AND TIME

DYNAMIC DNS SETTINGS

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

GENERAL

Current Date and Time: 2009-10-29 02:07:06

TIME ZONE AND DAYLIGHT SAVING TIME SETTINGS

Time zone:

Enable daylight saving time

Offset: minutes

Start Date:

End Date:

AUTOMATIC TIME SYNCHRONIZATION

Disabled

D-Link (pre-configured timesync server)

Custom

Time Server Type:

Primary Time Server: E.g. 'dns:ntp.domain.com'

Secondary Time Server: (optional)

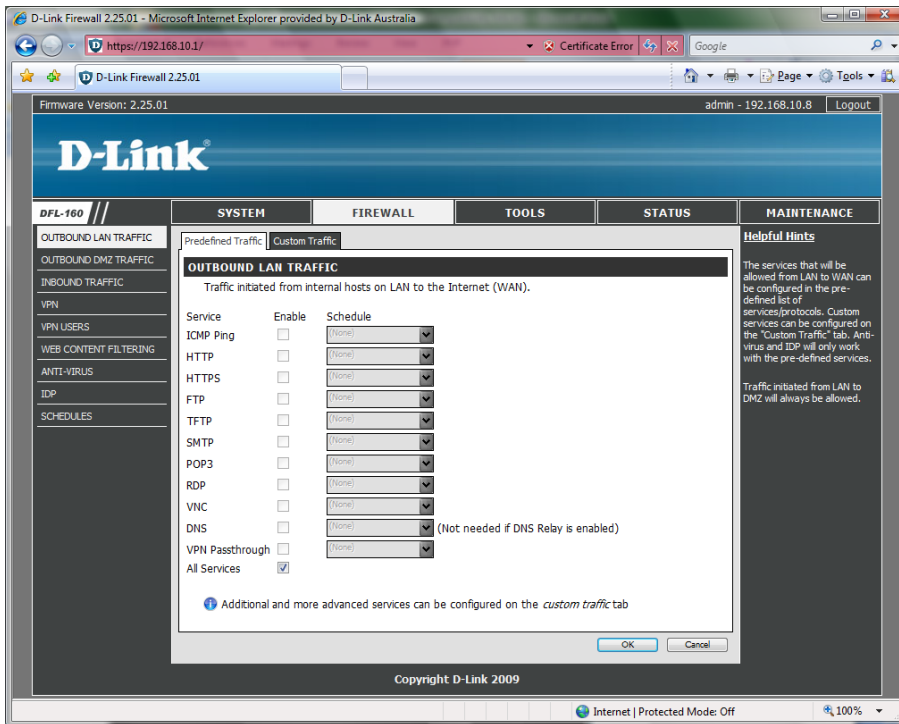
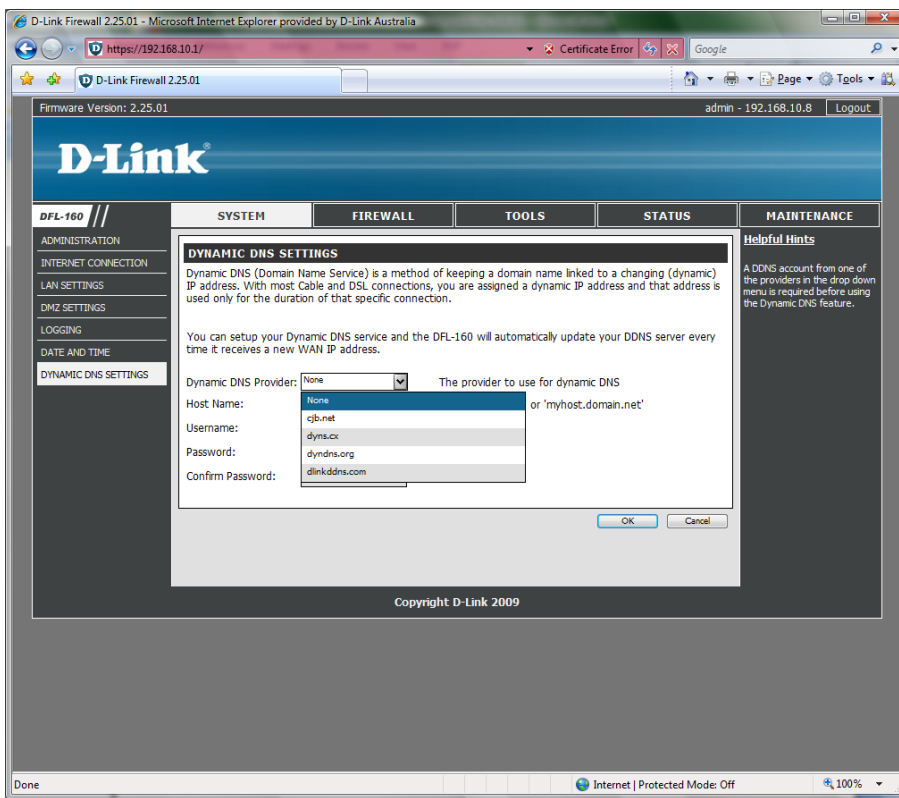
OK Cancel

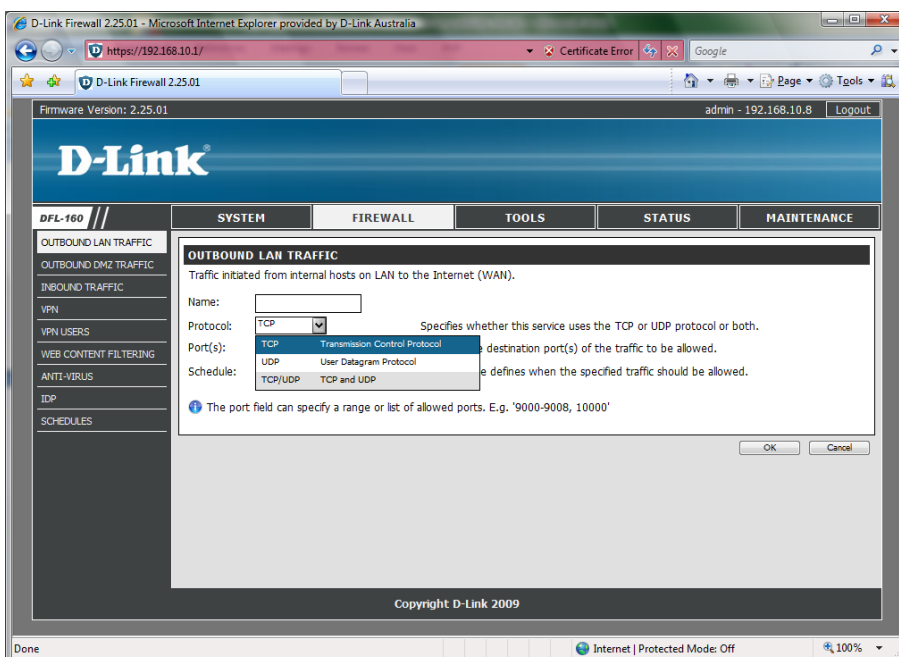
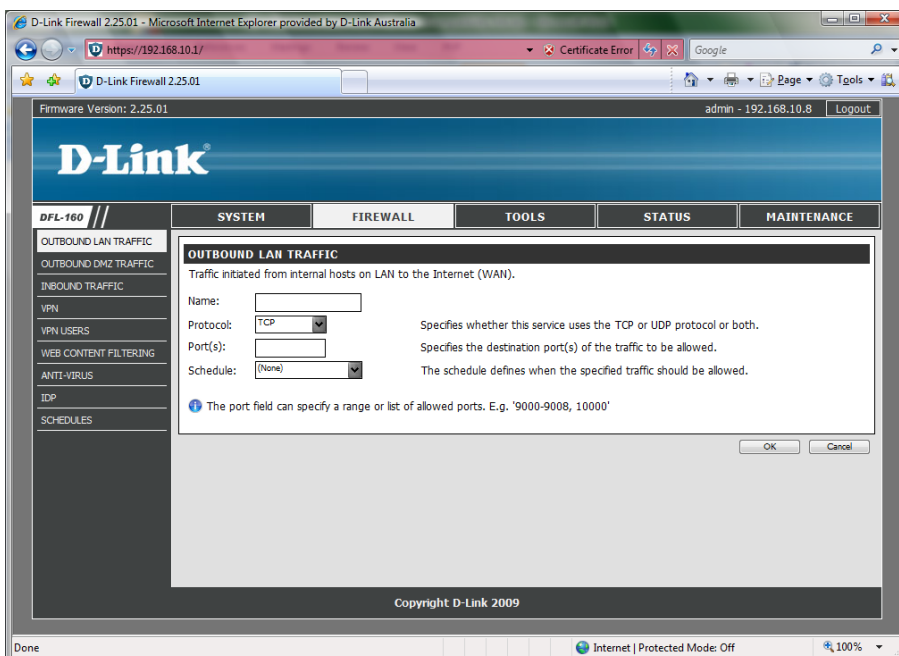
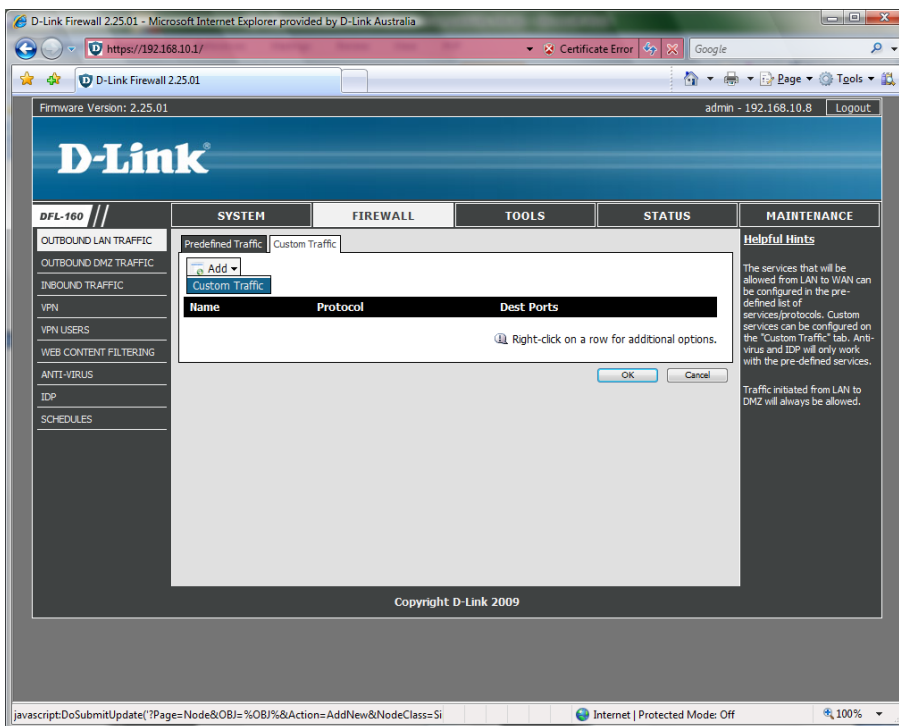
Copyright D-Link 2009

Helpful Hints

The date and time setting must be correct in order to use the scheduling feature. Log messages will report the wrong time for a triggered event if the date and time settings are incorrect. The firewall can automatically synchronize its time setting with an external time server on the Internet, if configured.

Internet | Protected Mode: Off 100%





D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

OUTBOUND LAN TRAFFIC

OUTBOUND DMZ TRAFFIC

INBOUND TRAFFIC

VPN

VPN USERS

WEB CONTENT FILTERING

ANTI-VIRUS

IDP

SCHEDULES

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

Predefined Traffic Custom Traffic

OUTBOUND DMZ TRAFFIC

Traffic initiated from internal hosts on DMZ to the Internet (WAN).

Service	Enable	Schedule
ICMP Ping	<input type="checkbox"/>	(None)
HTTP	<input type="checkbox"/>	(None)
HTTPS	<input type="checkbox"/>	(None)
FTP	<input type="checkbox"/>	(None)
TFTP	<input type="checkbox"/>	(None)
SMTP	<input checked="" type="checkbox"/>	(None)
POP3	<input type="checkbox"/>	Name Start End date date
RDP	<input type="checkbox"/>	(None)
VNC	<input type="checkbox"/>	NonWorkingHours
DNS	<input type="checkbox"/>	Weekdays (day is enabled)
VPN Passthrough	<input type="checkbox"/>	Weekends
All Services	<input type="checkbox"/>	WorkingHours

Additional and more advanced services can be configured on the *custom traffic* tab

Helpful Hints

The services that will be allowed and forwarded from DMZ to WAN can be configured in the pre-defined list of services/protocols. Custom services can be configured on the "Custom Traffic" tab. Anti-virus and IDP will only work with the pre-defined services.

Traffic initiated from DMZ to LAN will not be allowed.

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

OUTBOUND LAN TRAFFIC

OUTBOUND DMZ TRAFFIC

INBOUND TRAFFIC

VPN

VPN USERS

WEB CONTENT FILTERING

ANTI-VIRUS

IDP

SCHEDULES

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

Predefined Traffic Custom Traffic

INBOUND TRAFFIC

Traffic sent from the Internet to internal hosts on the LAN and DMZ.

Service	Enable	Server IP	Schedule	Details
HTTP	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 80
HTTPS	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 443
FTP	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 21
TFTP	<input type="checkbox"/>	192.168.11.10	(None)	UDP Port 69
SMTP	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 25
POP3	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 110
RDP	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 3389
VNC	<input type="checkbox"/>	192.168.11.10	(None)	TCP Port 5900
ICMP Ping	<input type="checkbox"/>	192.168.11.10		ICMP echo request

Additional and more complex services can be configured on the *custom traffic* tab

INBOUND MULTICAST

Multicast traffic can be forwarded to local clients on LAN and DMZ if the clients have requested the traffic using the IGMP protocol.

Allow requested multicast traffic

Multicast Groups: 224.0.0.251,225.0.0.251 Multicast groups to allow

Helpful Hints

The services that will be allowed and forwarded from WAN (Internet) to LAN and DMZ can be configured in the pre-defined list of services/protocols. Custom services can be configured on the "Custom Traffic" tab. Anti-virus and IDP will only work with the pre-defined services.

Make sure that the management ports for HTTP and HTTPS do not use the same port numbers as configured inbound traffic.

Enabling ICMP Ping will override and disable the WAN Ping on the Administration page.

OK Cancel

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- OUTBOUND LAN TRAFFIC
- OUTBOUND DMZ TRAFFIC
- INBOUND TRAFFIC**
- VPN
- VPN USERS
- WEB CONTENT FILTERING
- ANTI-VIRUS
- IDP
- SCHEDULES

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

INBOUND TRAFFIC

Traffic sent from the Internet to internal hosts on the LAN and DMZ.

Name:

Protocol: Specifies whether this service uses the TCP or UDP protocol or both.

Destination Port(s): Specifies the destination port(s) of the traffic to be forwarded.

Destination IP: Destination IP address of local server or host.

Schedule: The schedule defines when the specified traffic should be forwarded.

Change destination port(s) of incoming traffic to a local port different than the external port.
Local Destination Port(s): Specifies to which port(s) the traffic should be forwarded to on the local server or host.

i The port fields can specify a range of ports to be forwarded. E.g. '9000-9008'

OK Cancel

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- OUTBOUND LAN TRAFFIC
- OUTBOUND DMZ TRAFFIC
- INBOUND TRAFFIC
- VPN**
- VPN USERS
- WEB CONTENT FILTERING
- ANTI-VIRUS
- IDP
- SCHEDULES

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

VPN

emotelnetwork **RemoteGateway**

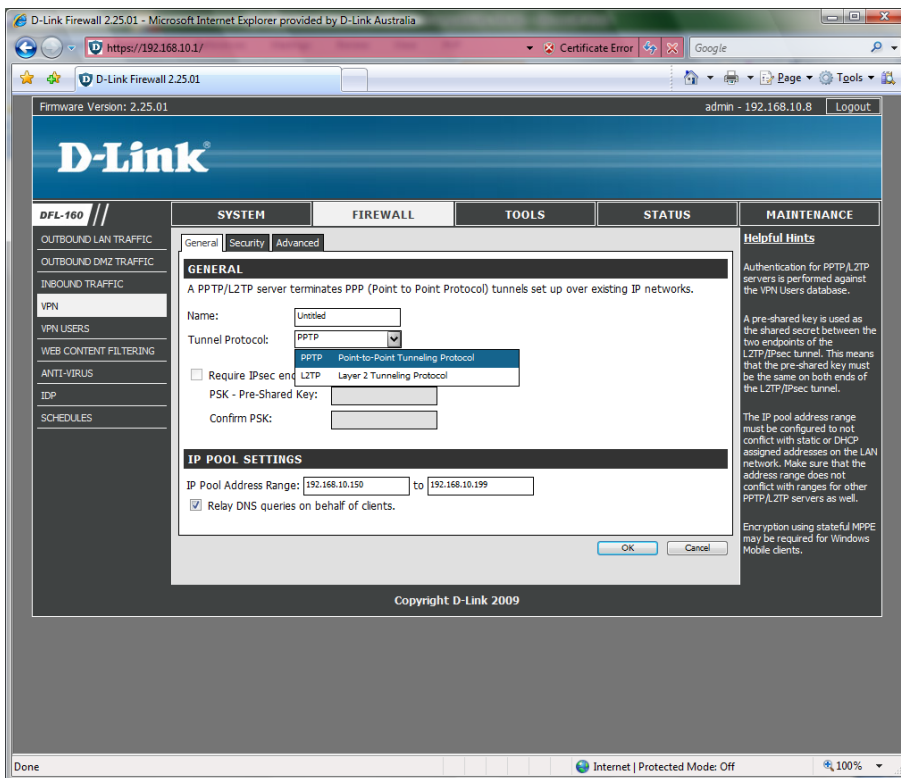
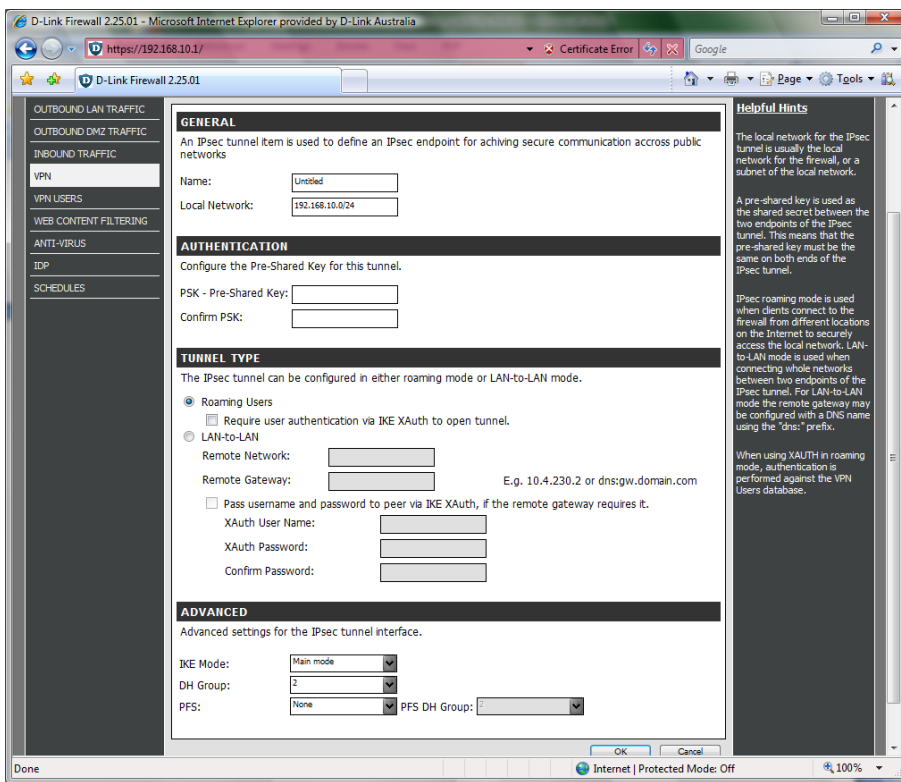
i Right-click on a row for additional options.

Helpful Hints

VPN (Virtual Private Network) can be used to securely connect over the public Internet to a protected network. The firewall supports IPsec, PPTP, and L2TP VPN. For more detailed information about configuring VPN in the firewall, please refer to the user manual.

Copyright D-Link 2009

https://192.168.10.1/?Page=Node&OBJ=/Firewall/VPN&Action=AddNew&NodeClass=Sim Internet | Protected Mode: Off 100%



D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- OUTBOUND LAN TRAFFIC
- OUTBOUND DMZ TRAFFIC
- INBOUND TRAFFIC
- VPN**
- VPN USERS
- WEB CONTENT FILTERING
- ANTI-VIRUS
- IDP
- SCHEDULES

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

General Security **Advanced**

AUTHENTICATION

- Allow un-authenticated users.
- Allow users to authenticate using PAP. (User name and password are sent in plaintext)
- Allow users to authenticate using CHAP.
- Allow users to authenticate using MS-CHAP. (MPPE Encryption Possible)
- Allow users to authenticate using MS-CHAP v2. (MPPE Encryption Possible)

MICROSOFT POINT-TO-POINT ENCRYPTION (MPPE)

- None
- RC4 40 bit
- RC4 56 bit
- RC4 128 bit
- Stateful MPPE (less secure, use only for compatibility)

OK Cancel

Copyright D-Link 2009

Helpful Hints

Authentication for PPTP/L2TP servers is performed against the VPN Users database.

A pre-shared key is used as the shared secret between the two endpoints of the L2TP/IPsec tunnel. This means that the pre-shared key must be the same on both ends of the L2TP/IPsec tunnel.

The IP pool address range must be configured to not conflict with static or DHCP assigned addresses on the LAN network. Make sure that the address range does not conflict with ranges for other PPTP/L2TP servers as well.

Encryption using stateful MPPE may be required for Windows Mobile clients.

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- OUTBOUND LAN TRAFFIC
- OUTBOUND DMZ TRAFFIC
- INBOUND TRAFFIC
- VPN**
- VPN USERS
- WEB CONTENT FILTERING
- ANTI-VIRUS
- IDP
- SCHEDULES

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

General Security **Advanced**

USER TIMEOUT

A user not sending any traffic for the specified timeout will be automatically disconnected.

Idle Timeout: seconds

OK Cancel

Copyright D-Link 2009

Helpful Hints

Authentication for PPTP/L2TP servers is performed against the VPN Users database.

A pre-shared key is used as the shared secret between the two endpoints of the L2TP/IPsec tunnel. This means that the pre-shared key must be the same on both ends of the L2TP/IPsec tunnel.

The IP pool address range must be configured to not conflict with static or DHCP assigned addresses on the LAN network. Make sure that the address range does not conflict with ranges for other PPTP/L2TP servers as well.

Encryption using stateful MPPE may be required for Windows Mobile clients.

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

VPN USERS

OUTBOUND LAN TRAFFIC

OUTBOUND DMZ TRAFFIC

INBOUND TRAFFIC

VPN

VPN USERS

WEB CONTENT FILTERING

ANTI-VIRUS

IDP

SCHEDULES

Helpful Hints

Clients connecting to the firewall via VPN (PPTP, L2TP, IPsec) will be authenticated using this database.

Right-click on a row for additional options.

Copyright D-Link 2009

https://192.168.10.1/?Page=Node&OBJ=/Firewall/VPNUsers# Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

GENERAL

Name:

Password:

Confirm Password:

OK Cancel

Helpful Hints

Make sure to configure a secure password that is not easy to guess.

Copyright D-Link 2009

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- OUTBOUND LAN TRAFFIC
- OUTBOUND DMZ TRAFFIC
- INBOUND TRAFFIC
- VPN
- VPN USERS
- WEB CONTENT FILTERING**
- ANTI-VIRUS
- IDP
- SCHEDULES

Dynamic Web Content Filtering | Static URL Filter

SUBSCRIPTION

License: No Subscription [Buy License](#) or [Enter License Key](#)

A service subscription is required before dynamic Web Content Filtering can be used.

WEB CONTENT FILTER

Enable Dynamic Web Content Filtering

When Web Content Filtering is enabled, all HTTP connections from LAN and DMZ to WAN will be checked if the content of the requested site is allowed.

CATEGORIES

FilteringCategories

Allowed	Blocked
<ul style="list-style-type: none"> Adult content Advertising Business oriented Chatrooms Clubs and Societies Computing/IT Crime/Terrorism Dating sites Drugs/Alcohol E-Banking 	

Non-Managed Action: **Allow** Action to take for content that hasn't been classified.

Allow users to override a *Restricted Site* notice and access blocked content.

Allow users to reclassify blocked content.

OK Cancel

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- OUTBOUND LAN TRAFFIC
- OUTBOUND DMZ TRAFFIC
- INBOUND TRAFFIC
- VPN
- VPN USERS
- WEB CONTENT FILTERING**
- ANTI-VIRUS
- IDP
- SCHEDULES

Dynamic Web Content Filtering | Static URL Filter

Web Content Filtering URL

Action	URL	Comments

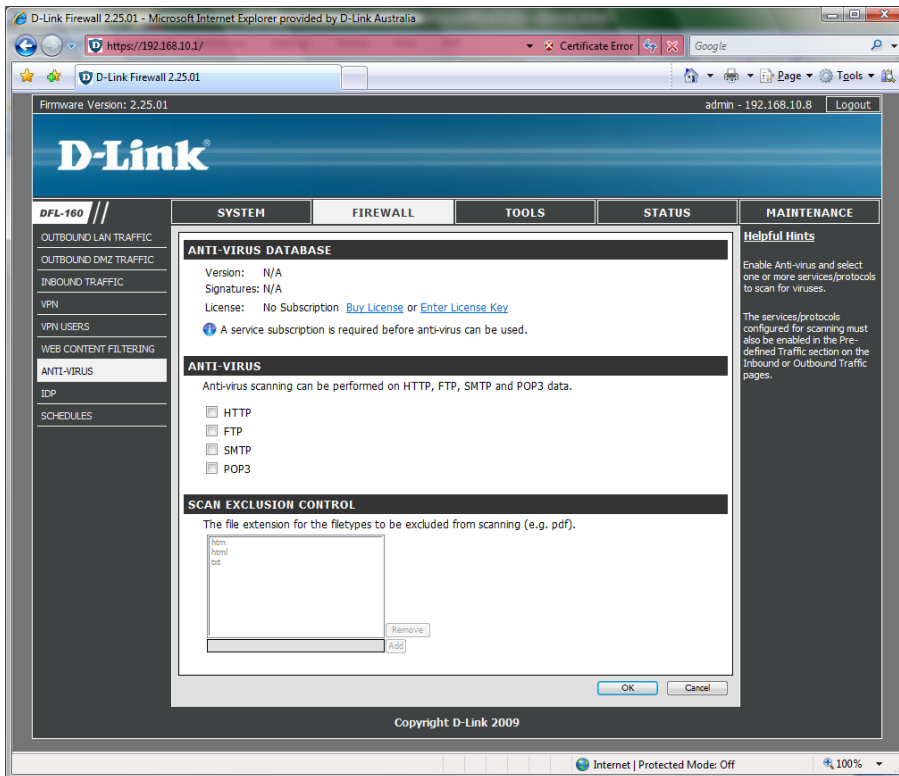
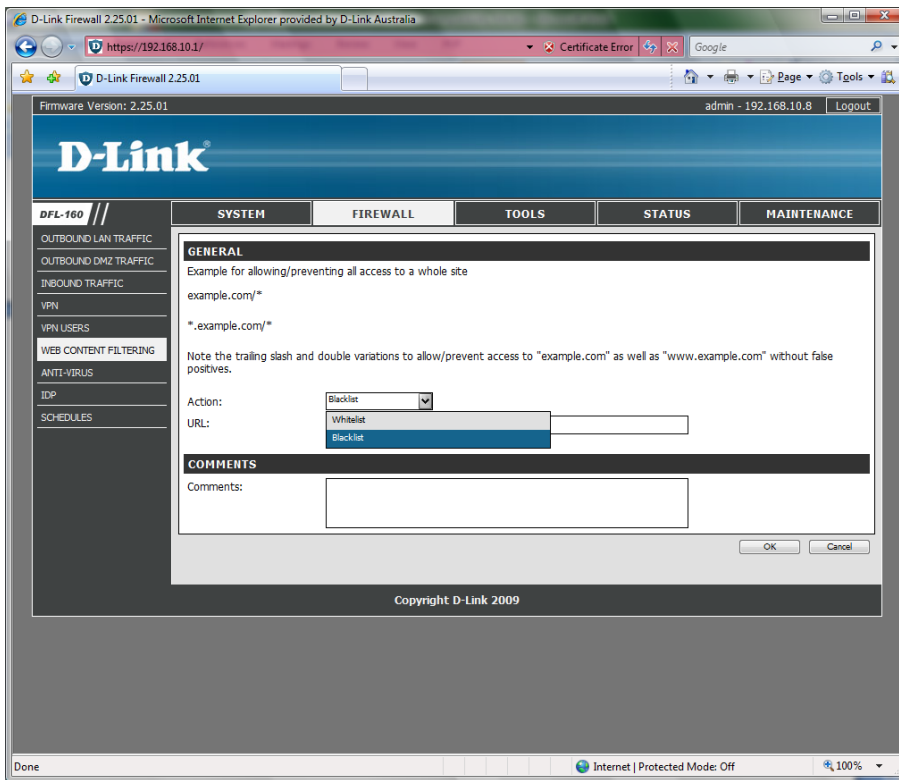
Right-click on a row for additional options.

OK Cancel

Copyright D-Link 2009

javascript:DoSubmitUpdate('?Page=Node&OBJ=%0B/%&Action=AddNew&NodeClass=SI

Internet | Protected Mode: Off 100%



D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

OUTBOUND LAN TRAFFIC
OUTBOUND DMZ TRAFFIC
INBOUND TRAFFIC
VPN
VPN USERS
WEB CONTENT FILTERING
ANTI-VIRUS
IDP
SCHEDULES

IDP DATABASE

Version: N/A
Signatures: N/A
License: No Subscription [Buy License](#) or [Enter License Key](#)
A service subscription is required before IDP can be used.

IDP - INTRUSION DETECTION AND PREVENTION

Select which mode the firewall should use. Detection will log that an attack has occurred, but still allow the traffic through the firewall. The prevention mode will both log the attack and drop the connection to protect your server.

Intrusion Detection (log only)
 Intrusion Prevention (log and drop connection)

Select protocols to protect. The firewall will scan traffic coming from WAN to LAN and DMZ on the ports/protocols selected below.

- HTTP (port 80) Protects an internal web server from attacks
- SMTP (port 25) Protects an internal mail server from attacks
- POP3 (port 110) Protects an internal POP3 client from attacks
- FTP (port 21) Protects an internal FTP server from attacks
- TFTP (port 69) Protects an internal TFTP server from attacks
- SSH (port 22) Protects internal SSH servers from attacks
- VoIP Protects internal voice over IP clients from attacks
- Remote Access Protects internal host with remote access like VNC from attacks
- Scanners Protects internal hosts from scanners
- Worms and Malware Protects internal hosts from worms and malware

OK Cancel

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

OUTBOUND LAN TRAFFIC
OUTBOUND DMZ TRAFFIC
INBOUND TRAFFIC
VPN
VPN USERS
WEB CONTENT FILTERING
ANTI-VIRUS
IDP
SCHEDULES

SCHEDULES

Add

Name	Start date	End date	Comments
NonWorkingHours			All hours, except Monday to Friday 08:00-17:00
Weekdays			Monday to Friday, 00:00-23:59
Weekends			Saturday and Sunday, 00:00-23:59
WorkingHours			Monday to Friday, 08:00-17:00

Right-click on a row for additional options.

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

PING

PING

IP Address: 192.168.11.1
Number of Packets: 4
Packet Size: 32
Send

Results of pinging to 192.168.11.1:

Seq	Roundtrip	TTL
0	10 ms	255
1	10 ms	255
2	10 ms	255
3	10 ms	255

4 packets transmitted, 4 packets received, 0% packet loss.
Round trip time average: 10 ms.

Helpful Hints
Use a ping test to confirm the availability of a host computer on the Internet or the local networks. Ping can also be used to check that the network setup is correct.

Copyright D-Link 2009

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160 // SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

PING

IP Address:

Number of Packets:

Packet Size:

4 packets transmitted, 0 packets received, **100%** packet loss.
Round trip time average: **0 ms**.

Helpful Hints

Use a ping test to confirm the availability of a host computer on the Internet or the local network. Ping can also be used to check that the network setup is correct.

Copyright D-Link 2009

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160 // SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

SYSTEM STATUS

LOGGING

ANTI-VIRUS

WEB CONTENT FILTERING

IDP

CONNECTIONS

INTERFACES

IPSEC

USER AUTHENTICATION

ROUTES

DHCP SERVER

System Resources

CPU Load

Throughput

Connections

Memory Usage

CPU Load: 0%

RAM: 28 / 128 MB

Connections: 31 / 6000

IPsec: 0 / 30

System Information

Model: DFL-160

System Time: 2009-10-29 02:02:08

Uptime: 0 days, 00:18:43

Configuration: Version 1

Firmware Version: 2.25.01.25-12081 Jul 1 2009

Last Restart: Unknown reason

Configuration Log: [more...](#)

Error(s): 0
Warning(s): 0

UTM Statistics

Top 5 Web Content Filtering Categories

■ N/A

(100%)

Total classification count: 0

UTM Information

AV Signatures: 0 Signatures
Last updated -

IDP Signatures: 0 Signatures
Last updated -

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- SYSTEM STATUS
- LOGGING
- ANTI-VIRUS
- WEB CONTENT FILTERING
- IDP
- CONNECTIONS
- INTERFACES
- IPSEC
- USER AUTHENTICATION
- ROUTES
- DHCP SERVER

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

Anti-virus is not enabled.

ANTI-VIRUS LOG

Time: From To

Source Destination

Interface:

IP Address:

Port:

Event: Action:

Severity: (Any) Category: (Any)

Free Text:

Search Reset

Internal Logging (1-0:0) Refresh Log Clear log

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
------	----------	-------------	------	-------	-----------	-----------	-------------	--------------

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- SYSTEM STATUS
- LOGGING
- ANTI-VIRUS
- WEB CONTENT FILTERING
- IDP
- CONNECTIONS
- INTERFACES
- IPSEC
- USER AUTHENTICATION
- ROUTES
- DHCP SERVER

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

Web content filtering is not enabled.

WEB CONTENT FILTERING LOG

Time: From To

Source Destination

Interface:

IP Address:

Port:

Event: Action:

Severity: (Any) Category: (Any)

Free Text:

Search Reset

Internal Logging (1-0:0) Refresh Log Clear log

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
------	----------	-------------	------	-------	-----------	-----------	-------------	--------------

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- SYSTEM STATUS
- LOGGING
- ANTI-VIRUS
- WEB CONTENT FILTERING
- IDP
- CONNECTIONS
- INTERFACES
- IPSEC
- USER AUTHENTICATION
- ROUTES
- DHCP SERVER

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

IDP is not enabled.

IDP / IPS STATUS

Time: From To

Source Destination

Interface:

IP Address:

Port:

Event: Action:

Severity: (Any) Category: (Any)

Free Text:

Search Reset

Internal Logging (1-0:0) Refresh Log Clear log

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
------	----------	-------------	------	-------	-----------	-----------	-------------	--------------

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

SYSTEM STATUS

LOGGING

ANTI-VIRUS

WEB CONTENT FILTERING

IDP

CONNECTIONS

INTERFACES

IPSEC

USER AUTHENTICATION

ROUTES

DHCP SERVER

FILTER STATE TABLE DISPLAY

Source: Destination:

IP Address:

Interface: Any Any

IP Protocol: Any

Port:

Apply

State table contents (max 100 entries)

State	Proto	Source	Destination	Timeout
FIN_RCVD	TCP	lan:192.168.10.8:64323	core:192.168.10.1:443	29
FIN_RCVD	TCP	lan:192.168.10.8:64311	core:192.168.10.1:443	0
FIN_RCVD	TCP	lan:192.168.10.8:64309	core:192.168.10.1:443	0
FIN_RCVD	TCP	lan:192.168.10.8:64313	core:192.168.10.1:443	2
FIN_RCVD	TCP	lan:192.168.10.8:64315	core:192.168.10.1:443	2
FIN_RCVD	TCP	lan:192.168.10.8:64317	core:192.168.10.1:443	16
FIN_RCVD	TCP	lan:192.168.10.8:64319	core:192.168.10.1:443	16
FIN_RCVD	TCP	lan:192.168.10.8:64321	core:192.168.10.1:443	23
FIN_RCVD	TCP	lan:192.168.10.8:64339	core:192.168.10.1:443	49
FIN_RCVD	TCP	lan:192.168.10.8:64341	core:192.168.10.1:443	65
FIN_RCVD	TCP	lan:192.168.10.8:64343	core:192.168.10.1:443	72

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

SYSTEM STATUS

LOGGING

ANTI-VIRUS

WEB CONTENT FILTERING

IDP

CONNECTIONS

INTERFACES

IPSEC

USER AUTHENTICATION

ROUTES

DHCP SERVER

INTERFACE STATUS

Interface: lan

IP Address: 192.168.10.1

Link Status: 1:100F 2:100F 3:100F 4:100F

MAC Address: 00-24-01-50-0f-41

Send Rate: 0 kbps

Receive Rate: 0 kbps

DRIVER INFORMATION / HARDWARE STATISTICS

```

IN : packets= 1611 bytes= 176475 errors= 0
OUT: packets= 903 bytes= 750704 errors= 0
In : Length Errors : 0
In : CRC Errors : 0
In : FIFO Overruns : 0
Out: Carrier Errors : 0
Out: FIFO Underruns : 0
Out: Late Collisions : 0
  
```

SEND RATE OVER THE PAST 24 HOURS

RECEIVE RATE OVER THE PAST 24 HOURS

Done

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- SYSTEM STATUS
- LOGGING
- ANTI-VIRUS
- WEB CONTENT FILTERING
- IDP
- CONNECTIONS
- INTERFACES
- IPSEC
- USER AUTHENTICATION
- ROUTES
- DHCP SERVER

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

IPSEC STATUS

IPsec Interface: [empty] [Let all active IKE SAs]

SEND RATE OVER THE PAST 24 HOURS

RECEIVE RATE OVER THE PAST 24 HOURS

IPSEC SAs

Remote Gateway	Local Net	Remote net	Protocol

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

- SYSTEM STATUS
- LOGGING
- ANTI-VIRUS
- WEB CONTENT FILTERING
- IDP
- CONNECTIONS
- INTERFACES
- IPSEC
- USER AUTHENTICATION
- ROUTES
- DHCP SERVER

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

USER AUTHENTICATION STATUS

Username	IP Address	Interface	Session Timeout	Idle Timeout	Logged in as	Forcibly Log Out

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

SYSTEM STATUS

LOGGING

ANTI-VIRUS

WEB CONTENT FILTERING

IDP

CONNECTIONS

INTERFACES

IPSEC

USER AUTHENTICATION

ROUTES

DHCP SERVER

ROUTING TABLE CONTENTS

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display:

Routing table contents (max 100 entries)					
Flags	Network	Interface	Gateway	Local IP	Metric
	192.168.10.0/24	lan			100
	192.168.11.0/24	dmz			100
	0.0.0.0/0	wan			100

In the "Flags" field of the routing tables, the following letters are used:
 O: Learned via OSPF X: Route is Disabled
 M: Route is Monitored A: Published via Proxy ARP
 D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

SYSTEM STATUS

LOGGING

ANTI-VIRUS

WEB CONTENT FILTERING

IDP

CONNECTIONS

INTERFACES

IPSEC

USER AUTHENTICATION

ROUTES

DHCP SERVER

DHCP SERVER STATUS

Name	Interface	IP Span	Usage		
DHCPsrvlan	lan	192.168.10.100-149	4%		<input type="button" value="Leases"/> <input type="button" value="Mappings"/>
DHCPsrvdmz	dmz	192.168.11.100-149	0%		<input type="button" value="Leases"/> <input type="button" value="Mappings"/>

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

UPDATE CENTER

LICENSE

BACKUP

RESET

UPGRADE

TECHNICAL SUPPORT

General Update Interval History

GENERAL

Current Firmware Version: 2.25.01.25-12081

[Click here](#) to go to D-Link's Security Portal to check for firmware updates

Automatic updates can be configured for each service by enabling the corresponding checkbox.

Enable	Service	Last Update	Status	Manual Update
<input type="checkbox"/>	Anti-virus	N/A	N/A	Update
<input type="checkbox"/>	Intrusion Detection & Prevention	N/A	N/A	Update

[Register at D-Link's Portal](#)

The update functionality for anti-virus and IDP requires valid subscriptions for the services. The firewall must be registered at D-Link's NetDefend Center prior to any updates are downloaded.

OK Cancel

Copyright D-Link 2009

Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

UPDATE CENTER

LICENSE

BACKUP

RESET

UPGRADE

TECHNICAL SUPPORT

General Update Interval History

TIMER SETTINGS

Update Interval: **Daily**

Every x Hour: **Daily**

Date in Month: **Weekly**

Day in Week: **Monthly**

Time of Day: 0 : 0 (HH:MM)

OK Cancel

Copyright D-Link 2009

Done Internet | Protected Mode: Off 100%

D-Link Firewall 2.25.01 - Microsoft Internet Explorer provided by D-Link Australia

https://192.168.10.1/ Certificate Error Google

D-Link Firewall 2.25.01

Firmware Version: 2.25.01 admin - 192.168.10.8 Logout

D-Link

DFL-160

SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

UPDATE CENTER

LICENSE

BACKUP

RESET

UPGRADE

TECHNICAL SUPPORT

General Update Interval History

GENERAL

Model Name: DFL-160

Issued Date: 2009-04-15 09:37:37

Last Modified: 2009-04-15 09:37:37

MAC Address: 00-24-01-50-0F-41

Active	Service	License	Expires
<input checked="" type="checkbox"/>	Anti-virus	N/A	N/A
<input checked="" type="checkbox"/>	Intrusion Detection & Prevention	N/A	N/A
<input checked="" type="checkbox"/>	Content Filtering	N/A	N/A

The activation codes for the included 12 month subscriptions for IDP, Antivirus and Web Content Filtering are provided after registration at [D-Link's NetDefend Center](#).

Additional 12 month subscriptions for these services can be purchased from your local D-Link dealer. You must have registered at the NetDefend Center before you submit an activation code.

- - - - [Activate](#)

LICENSE PROPERTIES

Connections: 6000

Rules: 300

IPsec Tunnels: 30

PPP Tunnels: 30

Internet | Protected Mode: Off 100%

