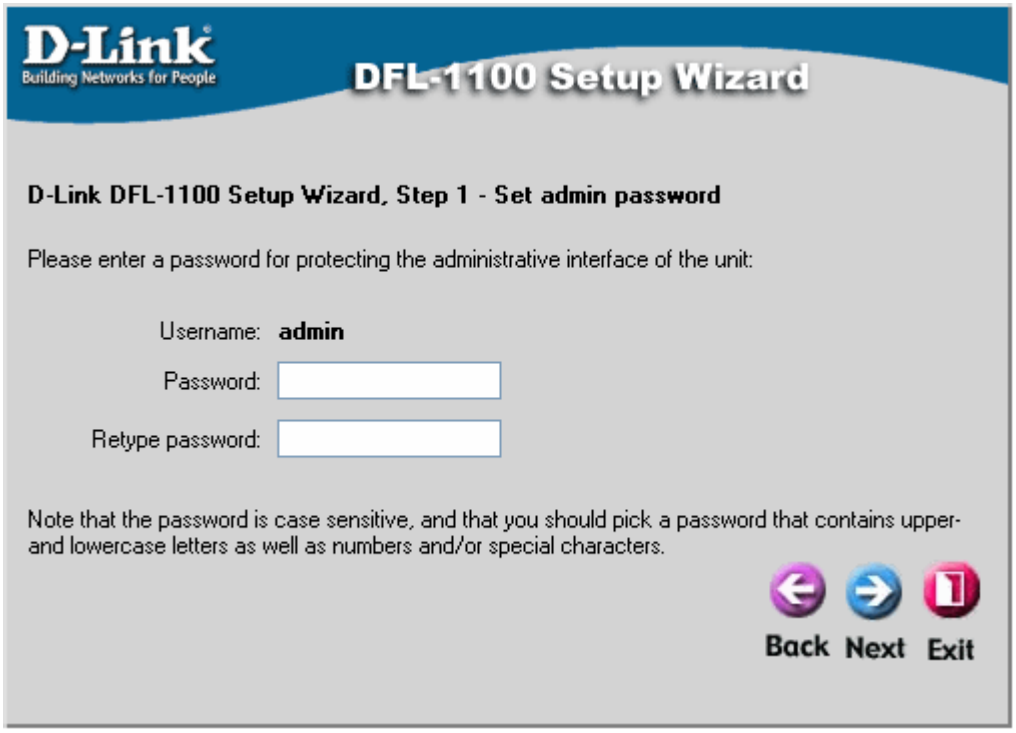
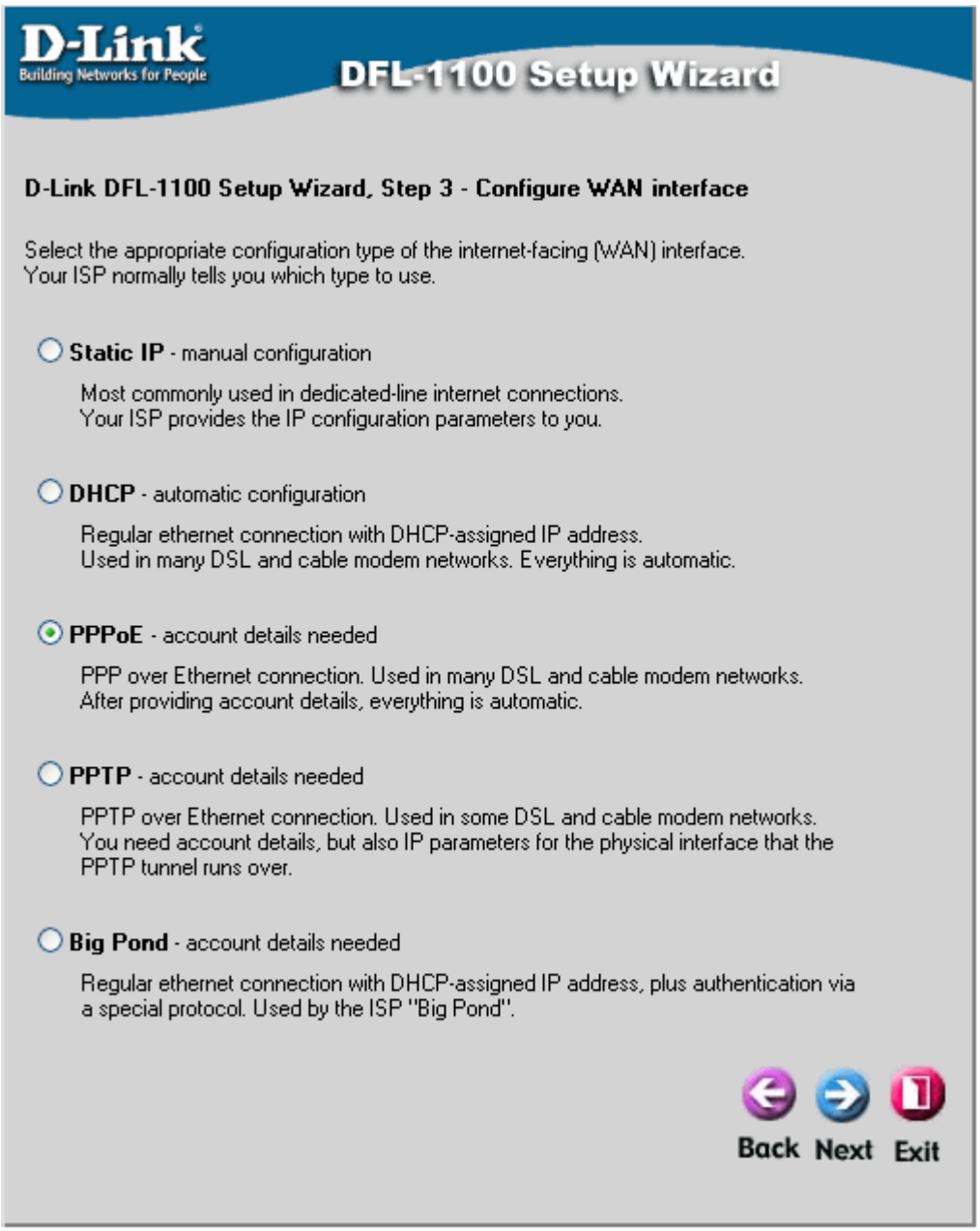
DFL-1100 Screenies

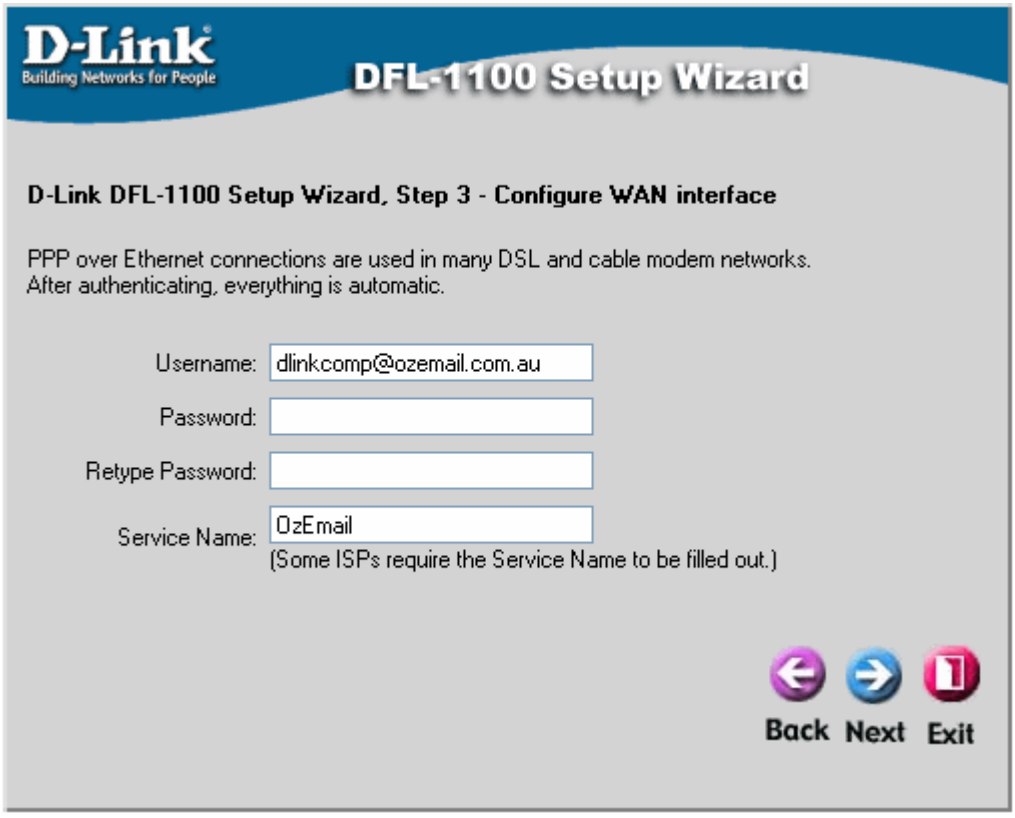
FW-1.20.00

Created By: Scott Howell

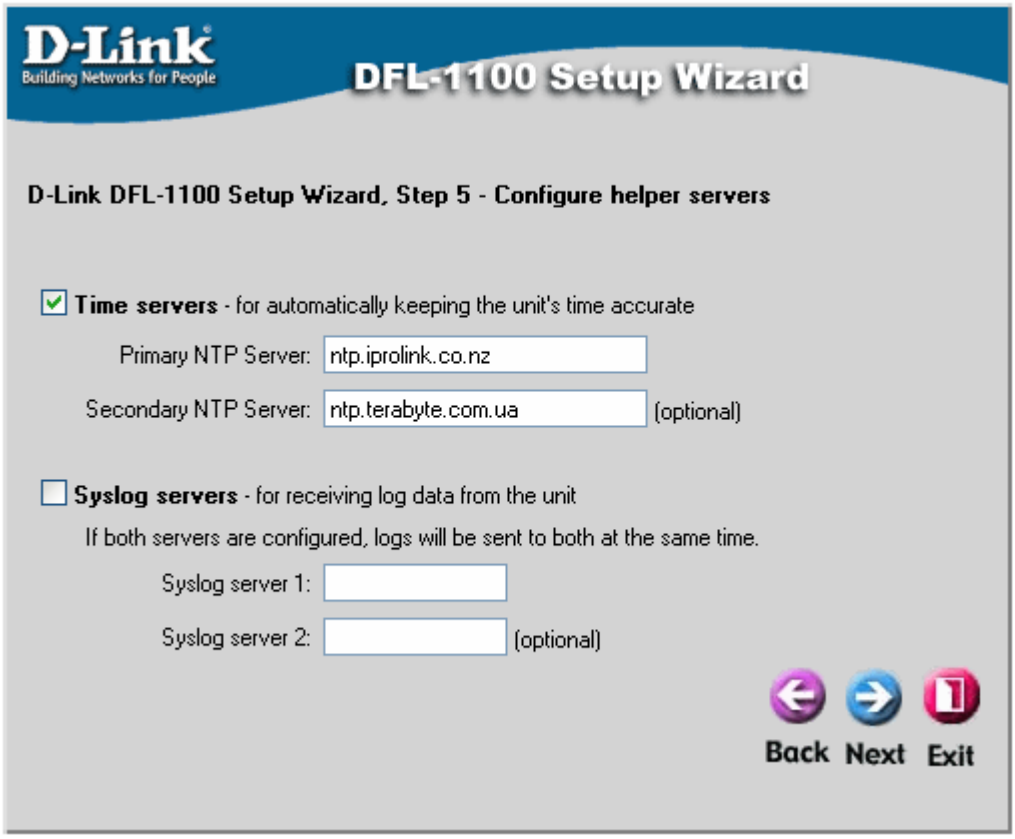

D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 1 - Set admin password
Please enter a password for protecting the administrative interface of the unit:
Username: admin
Password:
Retype password:
Note that the password is case sensitive, and that you should pick a password that contains upper- and lowercase letters as well as numbers and/or special characters.
Back
Next
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 2 - Set timezone
Select the appropriate time zone and click Next to continue.
(GMT+10:00) Canberra, Guam, Port Moresby, Vladivostok
Daylight saving time settings:
No daylight saving time
Apply daylight saving time from: Mar 28
... to: Oct 28
Back
Next
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface
Select the appropriate configuration type of the internet-facing (WAN) interface.
Your ISP normally tells you which type to use.
Static IP - manual configuration
Most commonly used in dedicated-line internet connections.
Your ISP provides the IP configuration parameters to you.
DHCP - automatic configuration
Regular ethernet connection with DHCP-assigned IP address.
Used in many DSL and cable modem networks. Everything is automatic.
PPPoE - account details needed
PPP over Ethernet connection. Used in many DSL and cable modem networks.
After providing account details, everything is automatic.
PPTP - account details needed
PPTP over Ethernet connection. Used in some DSL and cable modem networks.
You need account details, but also IP parameters for the physical interface that the
PPTP tunnel runs over.
Big Pond - account details needed
Regular ethernet connection with DHCP-assigned IP address, plus authentication via
a special protocol. Used by the ISP "Big Pond".
Back
Next
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface
PPP over Ethernet connections are used in many DSL and cable modem networks.
After authenticating, everything is automatic.
Username:
dlinkcomp@ozemail.com.au
Password:
Retype Password:
Service Name:
OzEmail
(Some ISPs require the Service Name to be filled out.)
Back
Next
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 4 - Set up built-in DHCP server
You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.
Disable DHCP Server
Enable DHCP Server
Enter a range of IP addresses to hand out to DHCP clients:
IP Range:
192.168.1.0 - 192.168.1.255
Back
Next
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 5 - Configure helper servers
Time servers - for automatically keeping the unit's time accurate
Primary NTP Server: ntp.iprolink.co.nz
Secondary NTP Server: ntp.terabyte.com.ua (optional)
Syslog servers - for receiving log data from the unit
If both servers are configured, logs will be sent to both at the same time.
Syslog server 1:
Syslog server 2: (optional)
Back
Next
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
D-Link DFL-1100 Setup Wizard Complete
Click Restart to finalize the configuration.
After the restart, the unit should be fully operational and use a basic firewall policy that allows nearly everything from the inside and out, and nothing in the opposite direction.
Back
Restart
Exit


D-Link
Building Networks for People
DFL-1100 Setup Wizard
The unit will now be restarted. This operation will take approximately 10 seconds, at which time you should be automatically transferred back to the main page of the web interface.
If you are not automatically transferred, you can reconnect to the unit manually.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Administration Settings

Management web GUI ports

HTTP Port: 80

HTTPS Port: 443

For security reasons, it may be better to run the management web GUI on non-standard ports. Also note that if web-based user authentication is enabled, ports 80 and 443 will be taken; the management web GUI has to use other ports.

Apply Cancel Help

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

Administrative access via **LAN** interface [Edit]

Ping: Any address
Admin: Any address (HTTPS only)

Add administrative access via:

Interface: WAN, DMZ, ETH4
VPN Tunnel:
VLAN Interface:

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Administration Settings

Edit administrative access via the **LAN** interface:

☑ **Ping** - standard ICMP echo to the IP address of the interface

Networks: _____ Blank = Any

☑ **Admin** - Full access to web-based management

Networks: _____ Blank = Any

Protocol: HTTPS only

☐ **Read-only** - Read-only access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **SNMP** - Simple Network Management Protocol (read-only access)

Networks: _____ Blank = Any

Community: _____

Note that you can specify multiple networks, e.g. "192.168.0.0/24, 10.0.0.5 - 10.0.0.9".

Apply Cancel Help

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

Administrative access via **LAN** interface [Edit]

Ping: Any address
Admin: Any address (HTTPS only)

Add administrative access via:

Interface: WAN, DMZ, ETH4
VPN Tunnel:
VLAN Interface:

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Administration Settings

Edit administrative access via the **WAN** interface:

☐ **Ping** - standard ICMP echo to the IP address of the interface

Networks: _____ Blank = Any

☐ **Admin** - Full access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **Read-only** - Read-only access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **SNMP** - Simple Network Management Protocol (read-only access)

Networks: _____ Blank = Any

Community: _____

Note that you can specify multiple networks, e.g. "192.168.0.0/24, 10.0.0.5 - 10.0.0.9".

Apply Cancel Help

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

Administrative access via **LAN** interface [Edit]

Ping: Any address
Admin: Any address (HTTPS only)

Add administrative access via:

Interface: WAN, DMZ, ETH4
VPN Tunnel:
VLAN Interface:

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Administration Settings

Edit administrative access via the **DMZ** interface:

☐ **Ping** - standard ICMP echo to the IP address of the interface

Networks: _____ Blank = Any

☐ **Admin** - Full access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **Read-only** - Read-only access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **SNMP** - Simple Network Management Protocol (read-only access)

Networks: _____ Blank = Any

Community: _____

Note that you can specify multiple networks, e.g. "192.168.0.0/24, 10.0.0.5 - 10.0.0.9".

Apply Cancel Help

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

Administrative access via **LAN** interface [Edit]

Ping: Any address
Admin: Any address (HTTPS only)

Add administrative access via:

Interface: WAN, DMZ, ETH4
VPN Tunnel:
VLAN Interface:

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Administration Settings

Edit administrative access via the **ETH4** interface:

☐ **Ping** - standard ICMP echo to the IP address of the interface

Networks: _____ Blank = Any

☐ **Admin** - Full access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **Read-only** - Read-only access to web-based management

Networks: _____ Blank = Any

Protocol: HTTP and HTTPS

☐ **SNMP** - Simple Network Management Protocol (read-only access)

Networks: _____ Blank = Any

Community: _____

Note that you can specify multiple networks, e.g. "192.168.0.0/24, 10.0.0.5 - 10.0.0.9".

Apply Cancel Help

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

Administrative access via **LAN** interface [Edit]

Ping: Any address
Admin: Any address (HTTPS only)

Add administrative access via:

Interface: WAN, DMZ, ETH4
VPN Tunnel:
VLAN Interface:

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Interface Settings

Pick an interface to edit from the below list:

Help

Available interfaces

LAN	[Edit]
WAN (PPPoE)	[Edit]
DMZ	[Edit]
ETH4	[Edit]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Interface Settings

Edit settings of the **LAN** interface:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Apply Cancel Help

Available interfaces

LAN	[Edit]
WAN (PPPoE)	[Edit]
DMZ	[Edit]
ETH4	[Edit]

Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type: PPPoE [Apply Change]

PPP over Ethernet connections are used in many DSL and cable modem networks.
After authenticating, everything is automatic.

Username: dlinkcomp@ozemail.com.au
Password: IIIII
Retype Password: IIIII
Service Name: OzEmail
(Some ISPs require the Service Name to be filled out.)

Most PPPoE services provide DNS server information. A few do not.
If this is the case, you can fill out their IP addresses yourself.

Primary DNS Server: (optional)
Secondary DNS Server: (optional)

☐ **Traffic shaping** - interface speed limits

In order to do traffic shaping beyond simple limits, such as guarantees and priorities, the traffic shaper needs to know what the maximum bandwidth is. Throughput through this interface will be limited to these speeds. If the limits are set too high, traffic shaping will not work.
These settings should match the speed of your Internet connection.

Upstream bandwidth: kbit/s
Downstream bandwidth: kbit/s

☐ **Manual Interface MTU Configuration** - maximum size of packets sent via this interface

Normally, you do not need to change the MTU settings. By default, the interface uses the maximum size that the physical media supports.

MTU: 1492 bytes. Upper limit: 1492.

Apply Cancel Help

Available interfaces

LAN [Edit]
WAN (PPPoE) [Edit]
DMZ [Edit]
ETH4 [Edit]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Interface Settings

Edit settings of the **DMZ** interface:

IP Address: 127.0.0.1

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Apply Cancel Help

Available interfaces

LAN	[Edit]
WAN (PPPoE)	[Edit]
DMZ	[Edit]
ETH4	[Edit]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Interface Settings

Edit settings of the **ETH4** interface:

IP Address: 127.0.0.1

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Apply Cancel Help

Available interfaces

LAN	[Edit]
WAN (PPPoE)	[Edit]
DMZ	[Edit]
ETH4	[Edit]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

VLAN Interfaces

Pick a VLAN interface to edit from the below list:

Help

Available VLAN interfaces

Name	Physical	VLAN ID

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

VLAN Interfaces

Edit settings of the **new** VLAN:

Name:	
Physical:	LAN
VLAN ID:	0 (0-4095)
IP Address:	
Subnet Mask:	255.255.255.0 - 256 hosts (/24)

Apply Cancel Help

Available VLAN interfaces

Name	Physical	VLAN ID

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Routing Table

Pick a route to edit from the below list:

Note that routing table ordering does not matter; smaller routes are always picked above larger ones.

Help

Routing table

Interface	Network	Gateway	Additional IP	Proxy ARP	
LAN	192.168.1.0/24				[Edit]
WAN	0.0.0.0/0				[Edit]
WAN	0.0.0.0/0				[Edit]
DMZ	127.0.0.0/24				[Edit]
ETH4	127.0.0.0/24				[Edit]

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Routing Table

Edit **192.168.1.0/255.255.255.0** route:

Note that this is the local network route for the interface; you can only change the Proxy ARP setting.

Interface: LAN

Network: 192.168.1.0

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Gateway: ☐ Network is behind remote gateway
0.0.0.0

Proxy ARP: ☐ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:
0.0.0.0

Apply Cancel Help

Routing table

Interface	Network	Gateway	Additional IP	Proxy ARP	
LAN	192.168.1.0/24				[Edit]
WAN	0.0.0.0/0				[Edit]
WAN	0.0.0.0/0				[Edit]
DMZ	127.0.0.0/24				[Edit]
ETH4	127.0.0.0/24				[Edit]

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Routing Table

Edit **0.0.0.0/0.0.0.0** route:

Note that this is the local network route for the interface; you can only change the Proxy ARP setting.

Interface: WAN

Network: 0.0.0.0

Subnet Mask: 0.0.0.0 - 4G hosts (/0)

Gateway: ☐ Network is behind remote gateway
0.0.0.0

Proxy ARP: ☐ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:
0.0.0.0

Apply Cancel Help

Routing table

Interface	Network	Gateway	Additional IP	Proxy ARP	
LAN	192.168.1.0/24				[Edit]
WAN	0.0.0.0/0				[Edit]
WAN	0.0.0.0/0				[Edit]
DMZ	127.0.0.0/24				[Edit]
ETH4	127.0.0.0/24				[Edit]

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Routing Table

Edit **127.0.0.0/255.255.255.0** route:

Note that this is the local network route for the interface; you can only change the Proxy ARP setting.

Interface: DMZ

Network: 127.0.0.0

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Gateway: ☐ Network is behind remote gateway
0.0.0.0

Proxy ARP: ☐ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:
0.0.0.0

Apply Cancel Help

Routing table

Interface	Network	Gateway	Additional IP	Proxy ARP	
LAN	192.168.1.0/24				[Edit]
WAN	0.0.0.0/0				[Edit]
WAN	0.0.0.0/0				[Edit]
DMZ	127.0.0.0/24				[Edit]
ETH4	127.0.0.0/24				[Edit]

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Routing Table

Edit **127.0.0.0/255.255.255.0** route:

Note that this is the local network route for the interface; you can only change the Proxy ARP setting.

Interface: DMZ

Network: 127.0.0.0

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Gateway: ☐ Network is behind remote gateway
0.0.0.0

Proxy ARP: ☐ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:
0.0.0.0

Apply Cancel Help

Routing table

Interface	Network	Gateway	Additional IP	Proxy ARP	
LAN	192.168.1.0/24				[Edit]
WAN	0.0.0.0/0				[Edit]
WAN	0.0.0.0/0				[Edit]
DMZ	127.0.0.0/24				[Edit]
ETH4	127.0.0.0/24				[Edit]

[Add new]

D-Link®
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

High Availability

Error:

High Availability setups may only be configured on units with static WAN connections.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Logging Settings

☐ **Syslog** - send log data via the syslog protocol to one or two servers

If both servers are configured, logs will be sent to both at the same time.

Syslog server 1:

Syslog server 2: (optional)

Syslog facility: Local0

☐ **Enable audit logging**

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

☐ **Enable E-mail alerting for IDS/IDP events**

Sensitivity: High

SMTP Server:

Sender:

E-Mail Address 1:

E-Mail Address 2:

E-Mail Address 3:

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

System | Firewall | Servers | Tools | Status | Help

Time Settings

Current time and date

☐ **Set the system time**

Date: 04 Aug 2004

Time: 01:02:20 (24 hour time)

Time zone and daylight saving time settings

Time zone: (GMT+10:00) Canberra, Guam, Port Moresby, Vladivostok

◉ No daylight saving time

○ Apply daylight saving time from: Jan 01

... to: Jan 01

Automatic time synchronization

☑ **Enable NTP**

Primary NTP Server: ntp.iprolink.co.nz

Secondary NTP Server: ntp.terabyte.com.ua (optional)

Note: The **Current time and date** and **Time zone** settings above will be applied instantly, and do not require **Activate Changes**.

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Select which policy to edit:

- Global policy parameters
- LAN->WAN policy - 4 rules, NAT enabled
- WAN->LAN policy - 0 rules
- LAN->DMZ policy - 3 rules
- DMZ->LAN policy - 0 rules
- WAN->DMZ policy - 0 rules
- DMZ->WAN policy - 4 rules, NAT enabled
- LAN->ETH4 policy - 0 rules
- ETH4->LAN policy - 0 rules
- WAN->ETH4 policy - 0 rules
- ETH4->WAN policy - 0 rules
- DMZ->ETH4 policy - 0 rules
- ETH4->DMZ policy - 0 rules

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Edit global policy parameters:

Fragments: ☐ Drop all fragmented packets

Minimum TTL: 3

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: **LAN->WAN** LAN->DMZ WAN->DMZ LAN->ETH4 WAN->ETH4 DMZ->ETH4
WAN->LAN DMZ->LAN DMZ->WAN ETH4->LAN ETH4->WAN ETH4->DMZ

Settings for LAN->WAN policy:

NAT:
- (•) Hide source addresses (many-to-one NAT)
- ( ) No NAT - requires public IP addresses on LAN network.

Apply Cancel Help

Select "Add New" below, or select a rule from the list to edit it:

LAN->WAN Policy

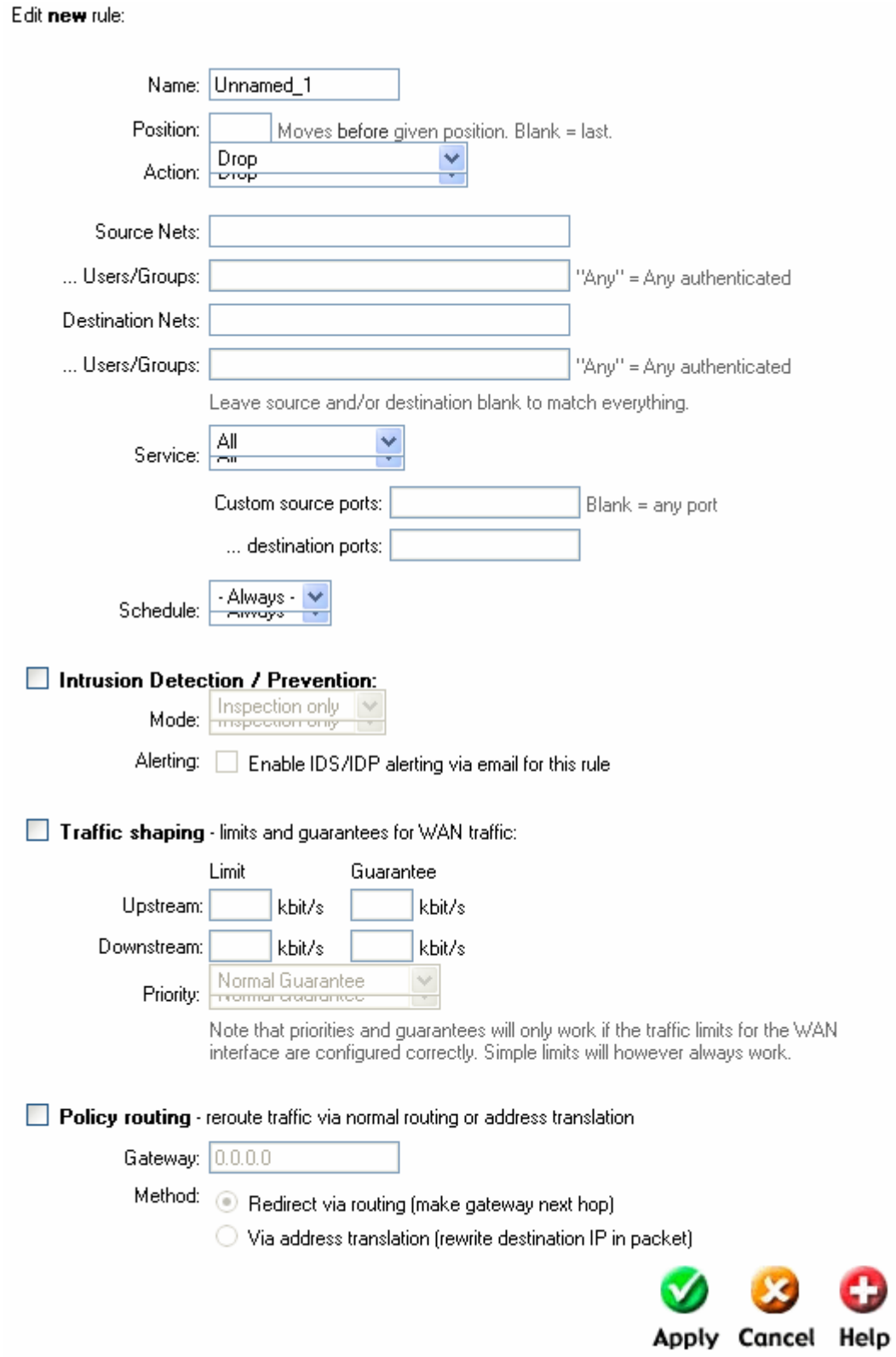
Name	Action	Source	Destination	Service	
#1 drop_smb-all	Drop	Any	Any	smb-all	[Edit]
#2 allow_ping-outbound	Allow	Any	Any	ping-outbound	[Edit]
#3 allow_ftp-passthrough	Allow	Any	Any	ftp-passthrough	[Edit]
#4 allow_standard	Allow	Any	Any	All Protocols	[Edit]

[Add new]

Order of evaluation

If no rule matches, the connection will be denied and logged.

Add New rule:


Edit **new** rule:
Name: Unnamed_1
Position: Moves before given position. Blank = last.
Action: Drop
Source Nets:
... Users/Groups: "Any" = Any authenticated
Destination Nets:
... Users/Groups: "Any" = Any authenticated
Leave source and/or destination blank to match everything.
Service: All
Custom source ports: Blank = any port
... destination ports:
Schedule: - Always -
Intrusion Detection / Prevention:
Mode: Inspection only
Alerting: Enable IDS/IDP alerting via email for this rule
Traffic shaping - limits and guarantees for WAN traffic:
Limit
Guarantee
Upstream: kbit/s kbit/s
Downstream: kbit/s kbit/s
Priority: Normal Guarantee
Note that priorities and guarantees will only work if the traffic limits for the WAN interface are configured correctly. Simple limits will however always work.
Policy routing - reroute traffic via normal routing or address translation
Gateway: 0.0.0.0
Method: Redirect via routing (make gateway next hop)
Via address translation (rewrite destination IP in packet)
Apply
Cancel
Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Note: Hosts on the LAN network are NATed. Writing rules that allow traffic from the Internet to hosts with private addresses will not work.

Select "Add New" below, or select a rule from the list to edit it:

WAN->LAN Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | **LAN->DMZ** | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Settings for LAN->DMZ policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

LAN->DMZ Policy

Name	Action	Source	Destination	Service	
#1 allow_ping-outbound	Allow	Any	Any	ping-outbound	[Edit]
#2 allow_ftp-passthrough	Allow	Any	Any	ftp-passthrough	[Edit]
#3 allow_standard	Allow	Any	Any	All Protocols	[Edit]

[Add new]

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | **DMZ->LAN** | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Settings for DMZ->LAN policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

DMZ->LAN Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | **WAN->DMZ** | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Note: Hosts on the DMZ network are NATed. Writing rules that allow traffic from the Internet to hosts with private addresses will not work.

Select "Add New" below, or select a rule from the list to edit it:

WAN->DMZ Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | **DMZ->WAN** | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Settings for DMZ->WAN policy:

NAT:
- (•) Hide source addresses (many-to-one NAT)
- ( ) No NAT - requires public IP addresses on DMZ network.

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

DMZ->WAN Policy

Name	Action	Source	Destination	Service	
#1 drop_smb-all	Drop	Any	Any	smb-all	[Edit]
#2 allow_ping-outbound	Allow	Any	Any	ping-outbound	[Edit]
#3 allow_ftp-passthrough	Allow	Any	Any	ftp-passthrough	[Edit]
#4 allow_standard	Allow	Any	Any	All Protocols	[Edit]

[Add new]

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | **LAN->ETH4** | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Settings for LAN->ETH4 policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

LAN->ETH4 Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | **ETH4->LAN** | ETH4->WAN | ETH4->DMZ

Settings for ETH4->LAN policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

ETH4->LAN Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | **WAN->ETH4** | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Select "Add New" below, or select a rule from the list to edit it:

WAN->ETH4 Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | DMZ->ETH4
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | **ETH4->WAN** | ETH4->DMZ

Settings for ETH4->WAN policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT - requires public IP addresses on ETH4 network.

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

ETH4->WAN Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN | LAN->DMZ | WAN->DMZ | LAN->ETH4 | WAN->ETH4 | **DMZ->ETH4**
WAN->LAN | DMZ->LAN | DMZ->WAN | ETH4->LAN | ETH4->WAN | ETH4->DMZ

Settings for DMZ->ETH4 policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT

Apply | Cancel | Help

Select "Add New" below, or select a rule from the list to edit it:

DMZ->ETH4 Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Firewall Policy

Show policy: LAN->WAN LAN->DMZ WAN->DMZ LAN->ETH4 WAN->ETH4 DMZ->ETH4
WAN->LAN DMZ->LAN DMZ->WAN ETH4->LAN ETH4->WAN **ETH4->DMZ**

Settings for ETH4->DMZ policy:

NAT:
- ○ Hide source addresses (many-to-one NAT)
- ◉ No NAT

Apply Cancel Help

Select "Add New" below, or select a rule from the list to edit it:

ETH4->DMZ Policy

Name	Action	Source	Destination	Service
[Add new]				

Order of evaluation

If no rule matches, the connection will be denied and logged.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Port Mapping / Virtual Servers

Select "Add New" to create a new port mapping, or select a mapping to edit from the below list:

Help

Configured mappings:

Name	Source	Destination	Service	Pass to

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

Port Mapping / Virtual Servers

Edit **new** mapping :

Name: Unnamed_1

Source Nets: Blank = everyone

... Users/Groups: "Any" = Any authenticated

Destination IP: Blank = WAN interface IP address

Service: Custom TCP

Custom source ports: Blank = any port

... destination ports:

... pass to port: ... and up. Blank=no change.

Pass To:

Schedule: - Always -

☐ **Intrusion Detection / Prevention:**

Mode: Inspection only

Alerting: ☐ Enable IDS/IDP alerting via email for this rule

☐ **Traffic shaping** - limits and guarantees for WAN traffic:

	Limit	Guarantee
Upstream:	kbit/s	kbit/s
Downstream:	kbit/s	kbit/s

Priority: Normal Guarantee

Note that priorities and guarantees will only work if the traffic limits for the WAN interface are configured correctly. Simple limits will however always work.

Apply Cancel Help

Configured mappings:

Name	Source	Destination	Service	Pass to

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

User Management

☐ **Enable User Authentication via HTTP / HTTPS**

HTTP Security: ◉ HTTP as well as HTTPS
○ HTTPS only

Idle Timeout: 2 hours

☐ **Enable RADIUS Support**

Primary Server: port 1812

Secondary Server: port 1812

Mode: PAP

Shared Secret:

Retype Secret:

RADIUS retry: 2 seconds

Apply Cancel Help

Select a user to edit from the below list, or select "Add new":

Administrative users

Admin: admin [Add]
Read-only: [Add]

Users in local database

User name **Groups**
[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

User Management

Edit user **admin**:

User name: admin

Group membership: administrators

☐ **Change password**

Password: |||||

Retype password: |||||

☐ **Delete user**

Membership in the "administrators" group means that the user can administer this unit.
Membership in the "auditors" group means that the user has read-only access to this unit.

Apply Cancel Help

Select a user to edit from the below list, or select "Add new":

Administrative users

Admin: admin [Add]
Read-only: [Add]

Users in local database

User name **Groups**
[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

User Management

Add new user:

User name:

Group membership:

Password:

Retype password:

Apply Cancel Help

Select a user to edit from the below list, or select "Add new":

Administrative users

Admin: admin [Add]
Read-only: [Add]

Users in local database

User name **Groups**
[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Manage Schedules

Pick a schedule to edit from the below list:

Help

Available schedules

Name	Start	Stop	Recurring

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

Manage Schedules

Edit **new** schedule:

Name:

Active from: 03 Aug 2004 Hour: 01

Active to: 04 Aug 2004 Hour: 01 (inclusive)

☐ **Recurring scheduling:**

	06:00	12:00	18:00
Mo:			
Tu:			
We:			
Th:			
Fr:			
Sa:			
Su:			

Apply Cancel Help

Defined schedules

Name	Start	Stop	Recurring

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

Services Settings

Pick a service to edit from the below list:

Help

Defined services

Name	Parameters	
igmp	IP Protocol: 2	[Edit]
rsvp	IP Protocol: 46	[Edit]
gre-encap	IP Protocol: 47	[Edit]
ipsec-esp	IP Protocol: 50	[Edit]
ipsec-ah	IP Protocol: 51	[Edit]
ipsec-natt	UDP: All -> 4500	[Edit]
ipip-encap	IP Protocol: 94	[Edit]
ipcomp	IP Protocol: 108	[Edit]
l2tp-encap	IP Protocol: 115	[Edit]
echo	TCP/UDP: All -> 7	[Edit]
chargen	TCP/UDP: All -> 19	[Edit]
ssh	TCP: All -> 22	[Edit]
ssh-in	TCP: All -> 22 SYN Relay	[Edit]
telnet	TCP: All -> 23	[Edit]
smtp	TCP: All -> 25	[Edit]
smtp-in	TCP: All -> 25 SYN Relay	[Edit]
time	TCP/UDP: All -> 37	[Edit]
dns-tcp	TCP: All -> 53	[Edit]
dns-udp	UDP: All -> 53	[Edit]
dns-all	TCP/UDP: All -> 53	[Edit]
bootps	UDP: All -> 67	[Edit]
bootpc	UDP: All -> 68	[Edit]
tftp	UDP: All -> 69	[Edit]
gopher	TCP: All -> 70	[Edit]
finger	TCP: All -> 79	[Edit]
http	TCP: All -> 80	[Edit]
https	TCP: All -> 443	[Edit]
http-in	TCP: All -> 80 SYN Relay	[Edit]
https-in	TCP: All -> 443 SYN Relay	[Edit]
http-outbound	TCP: All -> 80 ALG: "http-cf", max 100	[Edit]
pop3	TCP: All -> 110	[Edit]
sun-rpc	TCP: All -> 111	[Edit]
ident	TCP: All -> 113	[Edit]
nntp	TCP: All -> 119	[Edit]
ntp	TCP/UDP: All -> 123	[Edit]
epmap	TCP/UDP: All -> 135	[Edit]
netbios-name	UDP: All -> 137	[Edit]
netbios-dgm	UDP: All -> 138	[Edit]
netbios-ssn	TCP: All -> 139	[Edit]
microsoft-ds	TCP: All -> 445	[Edit]
imap	TCP: All -> 143	[Edit]
snmp	UDP: All -> 161	[Edit]
snmp-trap	UDP: All -> 162	[Edit]
ldap	TCP/UDP: All -> 389	[Edit]
ldaps	TCP: All -> 636	[Edit]

ike	UDP: All -> 500	[Edit]
rexec	TCP: All -> 512	[Edit]
rlogin	TCP: All -> 513	[Edit]
rcmd	TCP: All -> 514	[Edit]
syslog	UDP: All -> 514	[Edit]
lpr	TCP: All -> 515	[Edit]
ms-sql-s	TCP: All -> 1433	[Edit]
ms-sql-m	TCP/UDP: All -> 1434	[Edit]
wins	TCP/UDP: All -> 1512	[Edit]
l2tp-ctl	UDP: All -> 1701	[Edit]
pptp-ctl	TCP: All -> 1723	[Edit]
rdp	TCP: All -> 3389	[Edit]
radius	UDP: All -> 1812	[Edit]
radius-acct	UDP: All -> 1813	[Edit]
nfs-udp	UDP: All -> 2049	[Edit]
nfs-tcp	TCP: All -> 2049	[Edit]
nfs-all	TCP/UDP: All -> 2049	[Edit]
ping-outbound	ICMP: Echo (Ping) Return ICMP Errors	[Edit]
ping-inbound	ICMP: Echo (Ping)	[Edit]
traceroute-udp	UDP: All -> 33434-33499 Return ICMP Errors	[Edit]
ftp-inbound	TCP: All -> 21 ALG: "ftp-inbound", max 100	[Edit]
ftp-outbound	TCP: All -> 21 ALG: "ftp-outbound", max 100	[Edit]
ftp-passthrough	TCP: All -> 21 ALG: "ftp-passthrough", max 100	[Edit]
http-all	TCP: All -> 80, 443	[Edit]
http-in-all	TCP: All -> 80, 443 SYN Relay	[Edit]
smb-all	TCP/UDP: All -> 135-139, 445	[Edit]
ipsec-suite	Group: ipsec-esp, ipsec-ah, ike, ipsec-natt	[Edit]
l2tp-raw	Group: l2tp-ctl, l2tp-encap	[Edit]
l2tp-ipsec	Group: l2tp-ctl, ipsec-suite	[Edit]
pptp-suite	Group: gre-encap, pptp-ctl	[Edit]

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

Services Settings

Name:

TCP / UDP Service:

Protocol: TCP, UDP

Source Ports:

Destination Ports:

SYN Relay: Protect the destination from SYN flood attacks

ICMP Echo (Ping)

IP Protocol:

Protocols:

Example: "1-5, 9, 15, 50-51"

Group:

Services:

Comma-separated list of services or service groups.

Protocol-independent settings:

ICMP Errors: Allow ICMP errors from the destination to the source

ALG: -None-

Application Layer Gateways (ALGs) implement extra application logic that is needed for some protocols to work properly, like for instance FTP, which needs to open up dynamic data channels in addition to the command channel.

Max ALG Sessions: 100

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

VPN Tunnels

Pick a VPN tunnel to edit from the below list:

Help

VPN Tunnels

Name	Local Net	Remote Net	Remote Gateway

[Add new]

VPN Tunnels

Add VPN tunnel :

Name:

Local Net: 192.168.1.0/24

Authentication:

PSK - Pre-Shared Key

PSK:

Retype PSK:

Certificate-based

Local Identity: Admin - CN=000F3D59A840

Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)

Tunnel type:

Roaming Users - single-host VPN clients

IKE XAuth: Require user authentication via IKE XAuth to open tunnel.

LAN-to-LAN tunnel

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Proxy ARP: Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client: Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

VPN Tunnels

Name	Local Net	Remote Net	Remote Gateway

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

Manage Certificates

In order to do certificate-based authentication, first of all, you need to be able to identify yourself using a certificate to which you have the private key.

You also need:

- Copies of self-signed certificates of known peers, and/or
- One or more Certificate Authority certificates, and lists of identities that they have signed.

These aspects can all be configured through the below lists:

Help

Local identities (certificates to which you have the private key)

Name	Subject	Expires	Issuer	
Admin	CN=000F3D59A840	2031-04-14	CN=000F3D59A840	[Edit]

[Add new]

Certificates of remote peers

Name	Subject	Expires	Issuer

[Add new]

Certificate Authorities

Name	Subject	Expires	Issuer

[Add new]

Identities (lists of names signed by CAs)

List name	Members

[Add new]

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

HTTP Content Filtering

Changes to these settings affect services that use the "HTTP/HTML Content Filtering" ALG.
By default, this includes the "http-outbound" service.

Global Destination URL Whitelist:

URLs matching the global whitelist are excluded from all the below checks.

Contents: 10 entries

[Edit global URL whitelist]

Destination URL Blacklist:

Attempts to access URLs matching the blacklist is blocked.

Contents: 115 entries

[Edit URL blacklist]

Active content handling:

- ☐ Strip ActiveX objects (including Flash)
- ☐ Strip Java applets
- ☐ Strip Javascript/VBScript
- ☐ Block Cookies

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

HTTP Content Filtering

Edit Destination URL Global Whitelist:

To allow access to a whole domain, use e.g. "*.safesite.com/*". Note the ending slash, which protects against someone setting up e.g. "www.safesite.com.dyndnsprovider.net" as an alias for an otherwise disallowed site.

Blank lines are ignored. Lines beginning with "#" are also ignored.

```
# Access to sites that are important for software updates and
# require cookies / scripts:

d-link.com/*
*.d-link.com/*

dlink.com/*
*.dlink.com/*

d-link.com.tw/*
*.d-link.com.tw/*

dlink.com.tw/*
*.dlink.com.tw/*

microsoft.com/*
*.microsoft.com/*
```

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

System | Firewall | Servers | Tools | Status | Help

HTTP Content Filtering

Edit Destination URL Global Blacklist:

The URL blacklist can be used to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

Use e.g. "*example.org/*" to disallow access to an entire site.

Blank lines and lines beginning with "#" are ignored.

```
#
# Example for blocking all access to a whole site:
#
#   example.com/*
#   *.example.com/*
#
# Or, a shorter variant that runs the risk of blocking sites whose
# names end with the same text:
#
#   *example.com/*
#




#
# Deny access to potentially dangerous file types:
#

# Malicious executables can be downloaded by exploits
*.exe
*.scr
*.cpl
*.pif
# *.com   -- probably not a good idea given the .com TLD
```

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

DHCP Server

DNS Relay

System | Firewall | Servers | Tools | Status | Help

DHCP Server / Relaying Settings

Available interfaces

- LAN
- WAN
- DMZ
- ETH4

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

DHCP Server

DNS Relay

System | Firewall | Servers | Tools | Status | Help

DHCP Server / Relaying Settings

DHCP server / relaying settings for **LAN** interface:

- (•) **No DHCP processing**
  The unit will ignore DHCP requests heard on this interface.
- ( ) **Use built-in DHCP Server:**
  - IP Span:
  - DNS Servers: (optional)
    Use unit's own DNS relayer addresses
  - WINS Servers: (optional) (optional)
    WINS servers are used for name resolution in windows networks.
  - Domain name: (optional)
  - Lease time: 1 hour
    The gateway will be set to the IP address of the receiving interface.
- ( ) **Relay DHCP requests to other DHCP server:**
  - Server IP:

Apply Cancel Help

Available interfaces

LAN
WAN
DMZ
ETH4

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

DHCP Server

DNS Relay

System | Firewall | Servers | Tools | Status | Help

DNS Relay

The DNS Relayer can provide DNS service on up to two fixed local IP addresses.
These can be used as DNS servers by computers on the LAN.

☑ **Enable DNS Relayer**

IP Address 1: [ ]

☑ Use address of LAN interface

IP Address 2: [ ] (optional)

The requests will be relayed to the DNS servers that this unit itself uses.

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Ping
- DynDNS
- Backup
- Reset
- Upgrade

System | Firewall | Servers | Tools | Status | Help

Ping

IP Address:

Number of packets: 4

Packet size: 32

Apply Cancel Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Ping
- DynDNS
- Backup
- Reset
- Upgrade

Dynamic DNS Registration via HTTP

The unit can automatically register its external IP address with a DynDNS service so that it can be located via its DNS name. This is useful for e.g. VPN tunnels between gateways with dynamic IP addresses.

- (•) **Disabled**
- ( ) **cjb.net**
  - Username: [ ] (hostname becomes username.cjb.net)
  - Password: [ ]
- ( ) **dyns.cx**
  - Hostname: [.dyns.cx]
  - Username: [ ]
  - Password: [ ]
- ( ) **dyndns.org**
  - Hostname: [.dyndns.org]
  - Username: [ ]
  - Password: [ ]
- ( ) **Custom** - up to 3 HTTP requests, posted in sequence

  To use HTTP POST rather than GET, use "httppost://" rather than "http://".
  - URL 1: [ ]
  - URL 2: [ ]
  - URL 3: [ ]
  - Repeat: [1440] minutes

  Example: http://user:pass@svc.example.com/path?arg1=val1&arg2=val2

Apply | Cancel | Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Ping
- DynDNS
- Backup
- Reset
- Upgrade

System | Firewall | Servers | Tools | Status | Help

Backup / Restore

Backup unit's configuration

By clicking "Download configuration", you will receive a package file containing the unit's entire configuration. This can later be uploaded to the unit to restore the configuration.

Download configuration

Restore unit's configuration

To restore an old configuration, you can upload a previously downloaded backup file.

Browse...

Upload configuration

Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

- Ping
- DynDNS
- Backup
- Reset
- Upgrade

Restart / Reset

Restart

- (•) **Quick restart** - reset interfaces and re-read configuration
- ( ) **Full restart** - restart from power-on state

[Restart unit]

Reset to factory defaults

You can restore the unit to factory defaults. This means that all configuration parameters will be wiped, and all firmware upgrades removed.

On the next start-up, its LAN IP address will be 192.168.1.1, and the web GUI will begin with the setup wizard. It will not accept connections on any interface other than the LAN interface.

[Reset to Factory Defaults]

Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- Ping
- DynDNS
- Backup
- Reset
- Upgrade

System | Firewall | Servers | Tools | Status | Help

Upgrade

Upgrade unit's firmware

To upgrade the unit's firmware, download the firmware upgrade from the D-Link support web site and place it on your hard drive.

When the firmware is available, use this form to upload the new firmware to the unit. The unit will automatically be restarted to activate the new firmware.

Browse...

Upload firmware image

Upgrade unit's signature-database

To upgrade the unit's IDS signature-database, download the new signature database file from the D-Link support web site and place it on your hard drive.

When the signature file is available, use this form to upload it to the unit. After the new signature-database has been verified, the unit will automatically be restarted to activate the changes.

Browse...

Upload signature database

Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

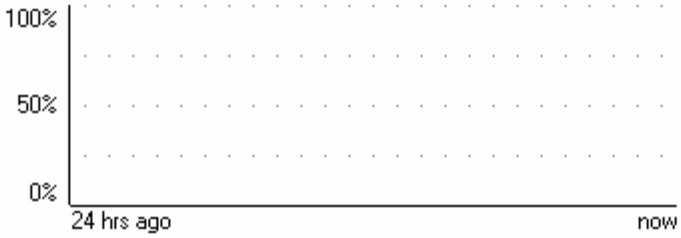
- System
- Interfaces
- VLAN
- VPN
- Connections
- DHCP Server

System | Firewall | Servers | Tools | Status | Help

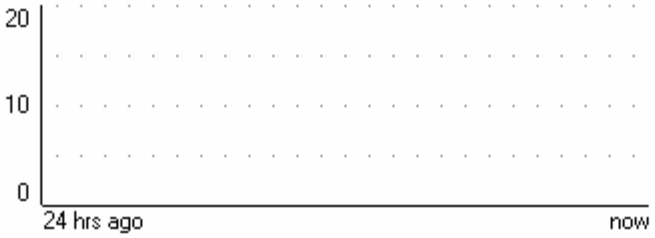
System Status

Uptime:	0 days, 00:49:58
Configuration:	Version 1, last changed at 2004-08-04 00:36:05 by "admin" from 192.168.1.231
CPU Load:	0%
Connections:	2 out of 200000 (0.0%)
Firmware version:	1.20.00
Last restart:	2004-08-04 00:36:06: Configuration generated by admin (192.168.1.231)
IDS Signatures:	Last changed at 2004-06-04 22:12:06

CPU load over the past 24 hours



State table usage over the past 24 hours



Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System
Interfaces
VLAN
VPN
Connections
DHCP Server

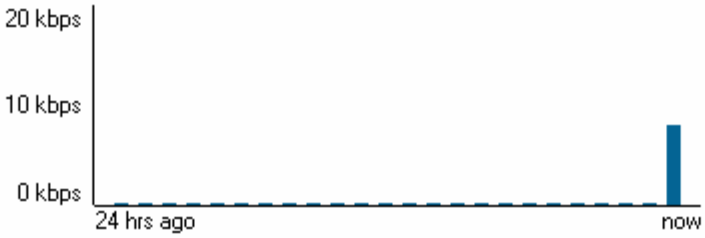
System | Firewall | Servers | Tools | Status | Help

Interface Status

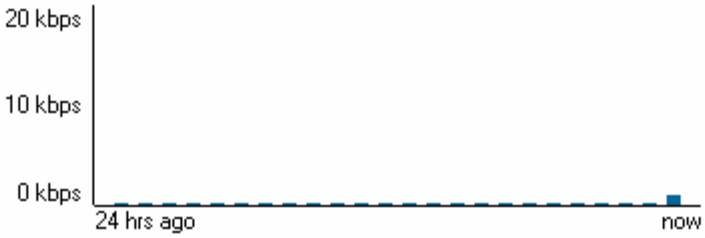
Interface: **LAN** WAN-PHYS WAN DMZ ETH4

Interface:	**LAN**
IP Address:	192.168.1.1
Link status:	100 Mbps Full Duplex
MAC Address:	000f:3d59:a842
Send rate:	8 kbps
Receive rate:	1 kbps

Send rate over the past 24 hours



Receive rate over the past 24 hours



Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- System
- Interfaces
- VLAN
- VPN
- Connections
- DHCP Server

System | Firewall | Servers | Tools | Status | Help

VLAN Interface Status

VLAN Interface: There are no VLAN interfaces configured

Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- System
- Interfaces
- VLAN
- VPN
- Connections
- DHCP Server

System | Firewall | Servers | Tools | Status | Help

VPN Status

No VPN tunnels have been configured.

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System
Interfaces
VLAN
VPN
Connections
DHCP Server

System | Firewall | Servers | Tools | Status | Help

State Table Contents

Filter state table display:

	Source	Destination
IP Address:		
Interface:	Any	Any
IP Protocol	Any	
Port:		

Any
Core
LAN
WAN
DMZ
ETH4

Apply Help

State table contents (max 100 entries)

State	Proto	Source	Destination	Timeout
FIN_RCVD	TCP	LAN:192.168.1.231:1825	core:192.168.1.1:443	2
TCP_OPEN	TCP	LAN:192.168.1.231:1828	core:192.168.1.1:443	262144

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

- System
- Interfaces
- VLAN
- VPN
- Connections
- DHCP Server

System | Firewall | Servers | Tools | Status | Help

DHCP Server Status

Interface: LAN WAN DMZ ETH4

Interface: **LAN**
IP Span: N/A

Help

D-Link
Building Networks for People

DFL-1100
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

Help

System
- Administration
- Interfaces
- VLAN
- Routing
- HA
- Logging
- Time

Firewall
- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

Servers
- DHCP Server
- DNS Relay

Tools
- Ping
- DynDNS
- Backup
- Reset
- Upgrade

Status
- System
- Interfaces
- VLAN
- HA
- VPN
- Connections
- DHCP Servers