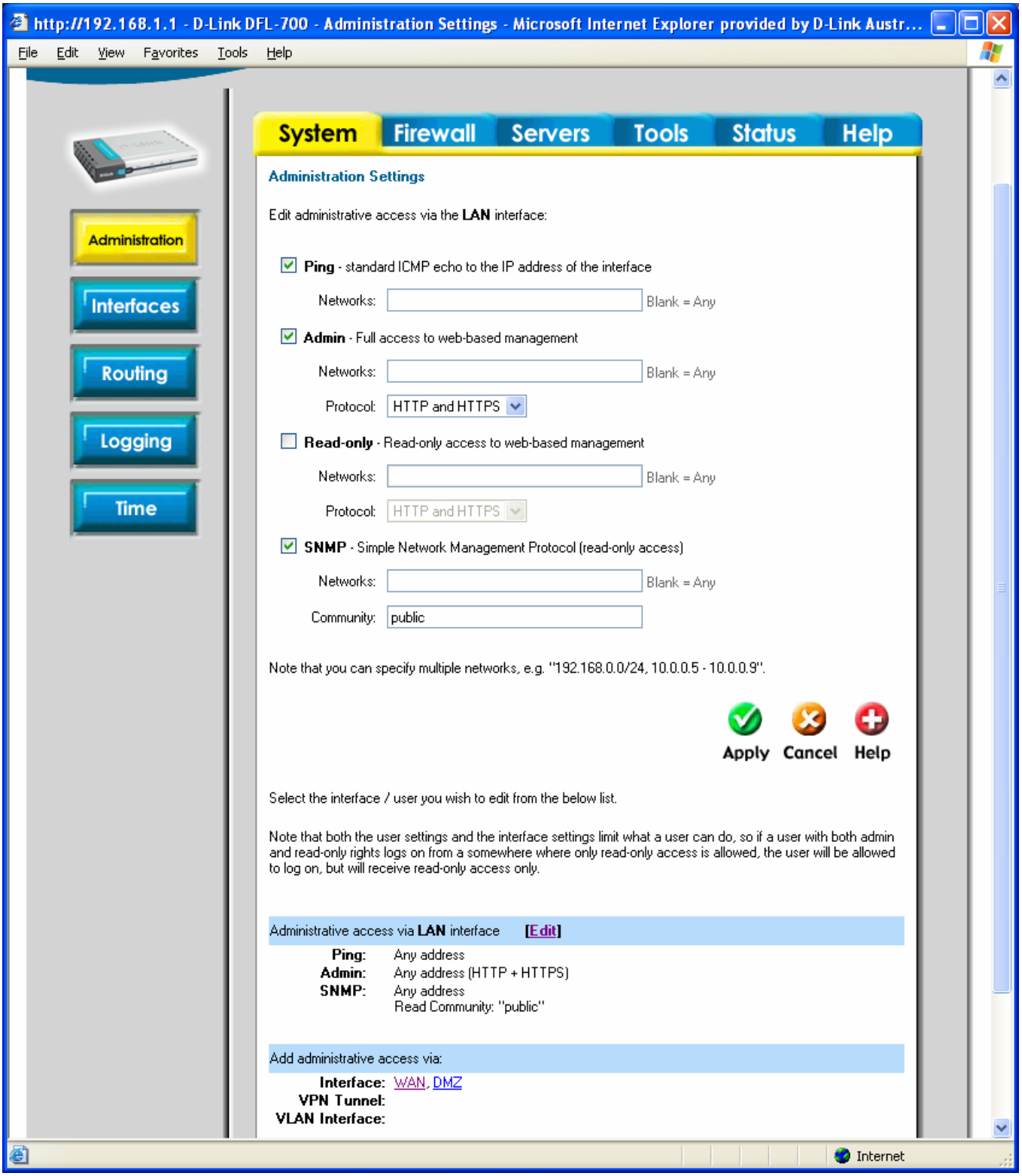
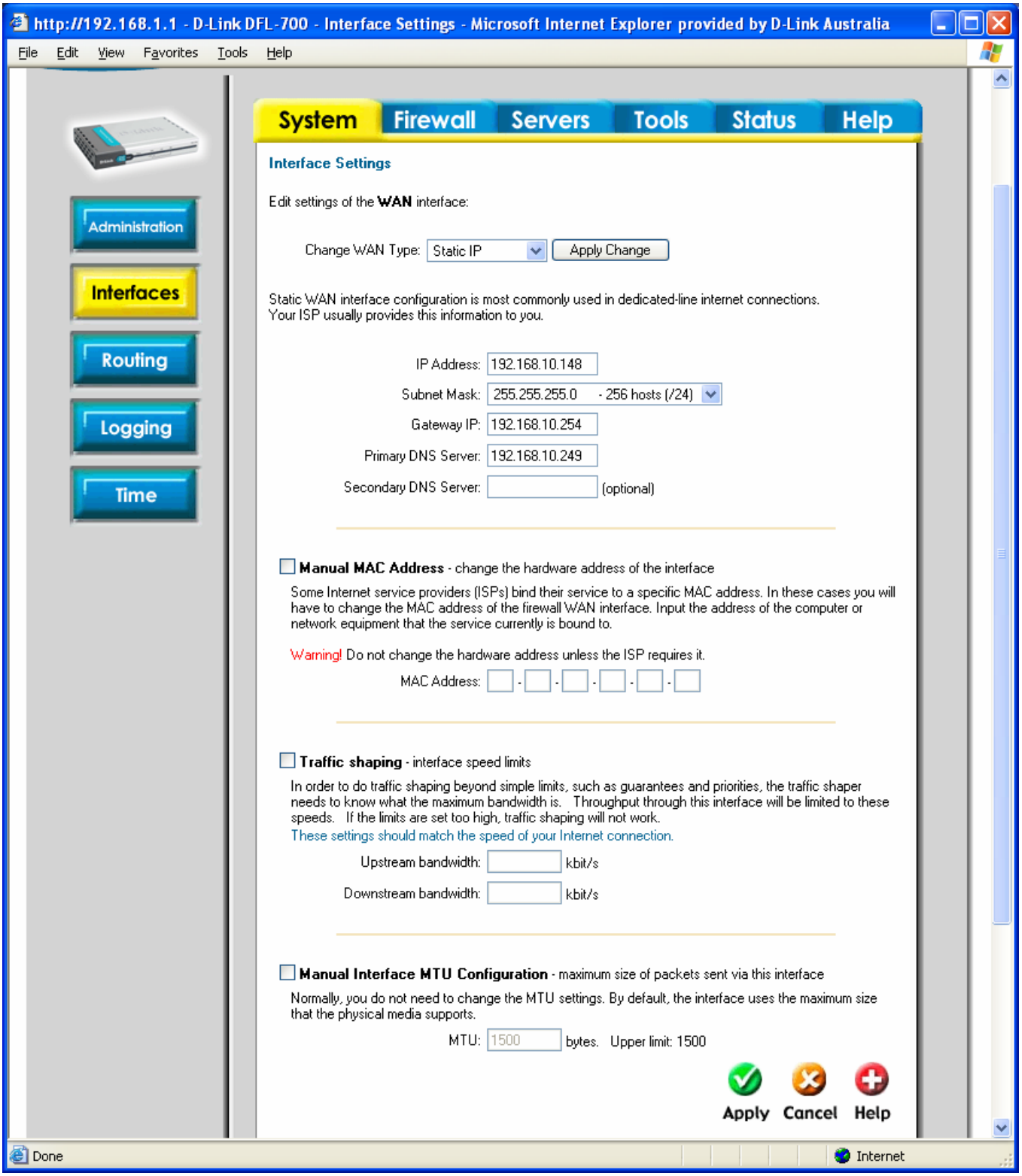

http://192.168.1.1 - D-Link DFL-700 - Administration Settings - Microsoft Internet Explorer provided by D-Link Austr...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
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 (HTTP + HTTPS)
SNMP: Any address
Read Community: "public"
Add administrative access via:
Interface: WAN, DMZ
VPN Tunnel:
VLAN Interface:
Internet

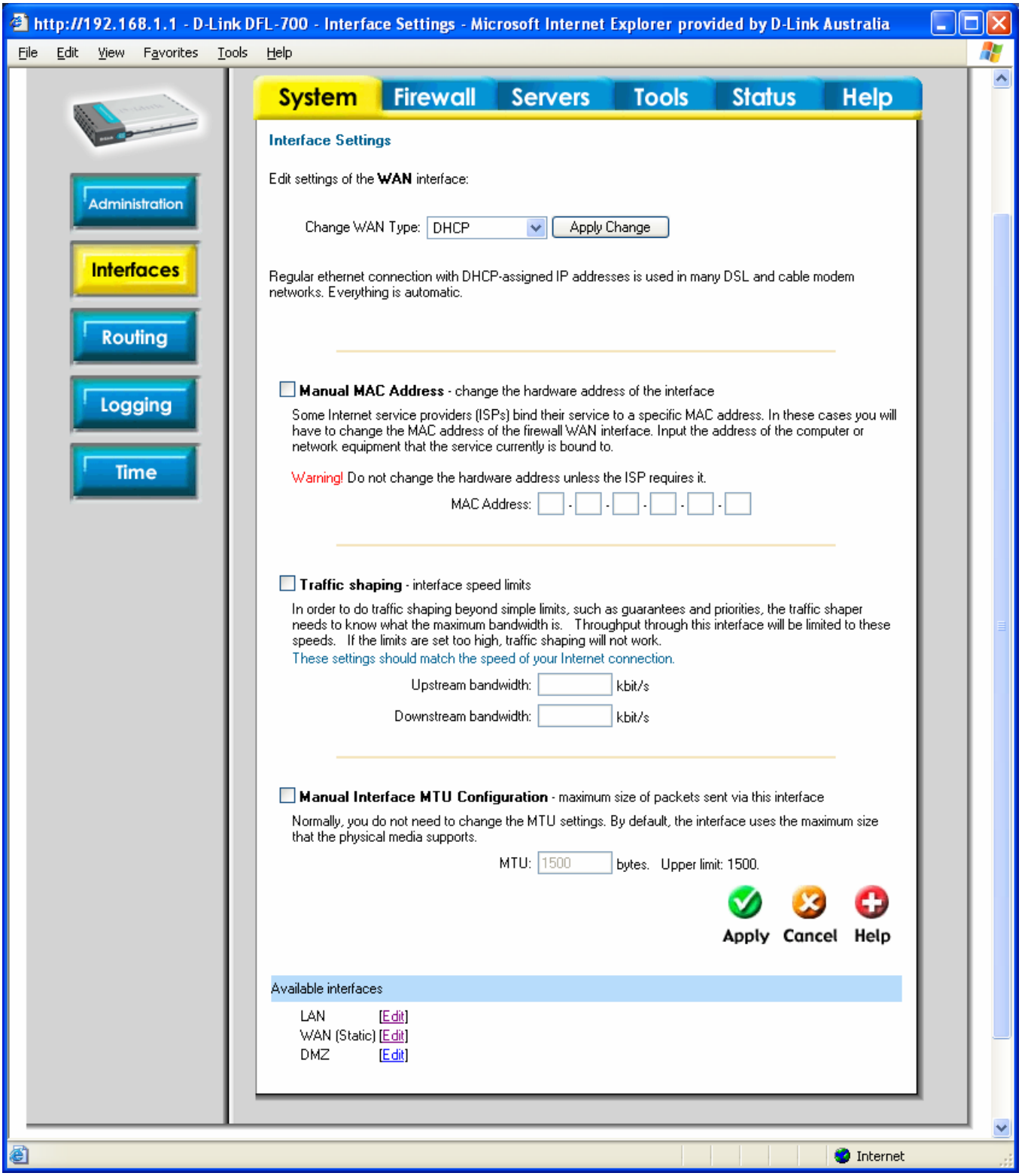

http://192.168.1.1 - D-Link DFL-700 - Administration Settings - Microsoft Internet Explorer provided by D-Link Austr...
File Edit View Favorites Tools Help
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Administration Settings
Edit administrative access via the 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: 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: public
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 (HTTP + HTTPS)
SNMP: Any address
Read Community: "public"
Add administrative access via:
Interface: WAN, DMZ
VPN Tunnel:
VLAN Interface:
Internet

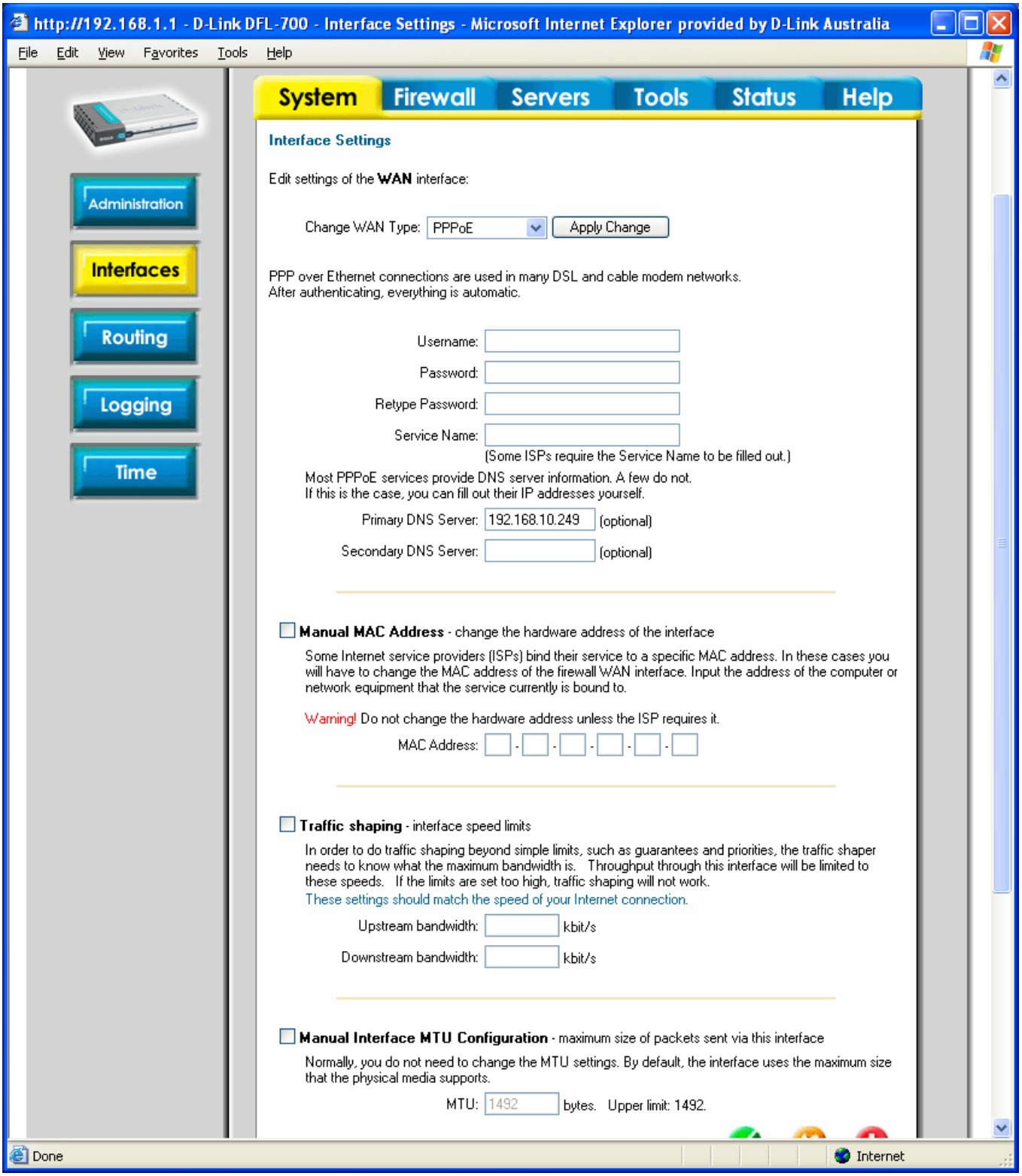

http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Firewall
Servers
Tools
Status
Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Pick an interface to edit from the below list:
Help
Available interfaces
LAN [Edit]
WAN (Static) [Edit]
DMZ [Edit]
Internet

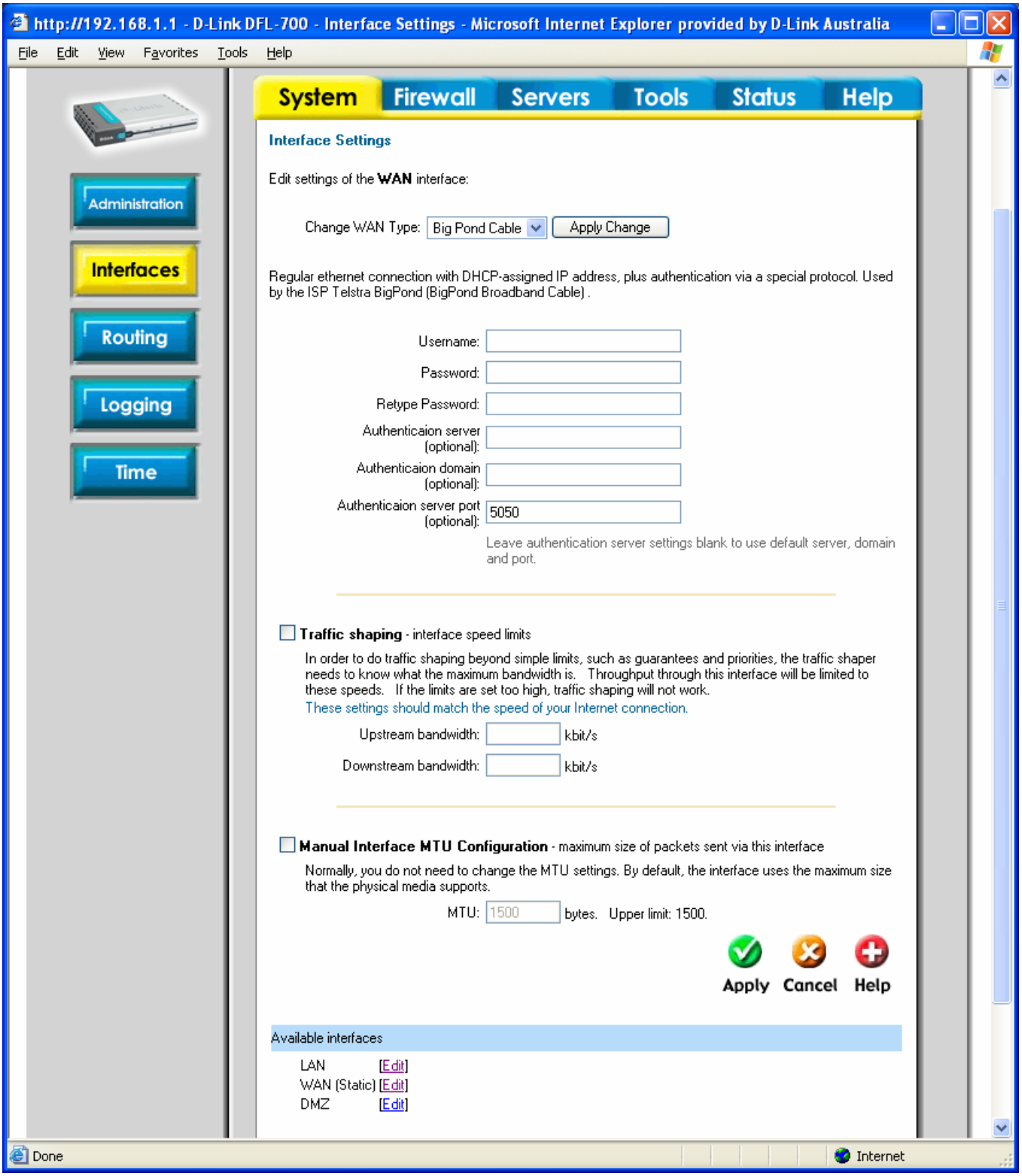

http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Edit settings of the LAN interface:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0 - 256 hosts (/24)
255.255.255.248 - 8 hosts (/29)
255.255.255.240 - 16 hosts (/28)
255.255.255.224 - 32 hosts (/27)
255.255.255.192 - 64 hosts (/26)
255.255.255.128 - 128 hosts (/25)
255.255.255.0 - 256 hosts (/24)
255.255.254.0 - 512 hosts (/23)
255.255.252.0 - 1k hosts (/22)
255.255.248.0 - 2k hosts (/21)
255.255.240.0 - 4k hosts (/20)
255.255.224.0 - 8k hosts (/19)
255.255.192.0 - 16k hosts (/18)
255.255.128.0 - 32k hosts (/17)
255.255.0.0 - 64k hosts (/16)
255.254.0.0 - 128k hosts (/15)
255.252.0.0 - 256k hosts (/14)
255.248.0.0 - 512k hosts (/13)
255.240.0.0 - 1M hosts (/12)
255.224.0.0 - 2M hosts (/11)
255.192.0.0 - 4M hosts (/10)
255.128.0.0 - 8M hosts (/9)
255.0.0.0 - 16M hosts (/8)
254.0.0.0 - 32M hosts (/7)
252.0.0.0 - 64M hosts (/6)
248.0.0.0 - 128M hosts (/5)
240.0.0.0 - 256M hosts (/4)
224.0.0.0 - 512M hosts (/3)
192.0.0.0 - 1G hosts (/2)
128.0.0.0 - 2G hosts (/1)
0.0.0.0 - 4G hosts (/0)
Apply Cancel Help
Available interfaces
LAN
WAN (Static)
DMZ
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Edit settings of the LAN interface:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0 - 256 hosts (/24)
255.255.255.248 - 8 hosts (/29)
255.255.255.240 - 16 hosts (/28)
255.255.255.224 - 32 hosts (/27)
255.255.255.192 - 64 hosts (/26)
255.255.255.128 - 128 hosts (/25)
255.255.255.0 - 256 hosts (/24)
255.255.254.0 - 512 hosts (/23)
255.255.252.0 - 1k hosts (/22)
255.255.248.0 - 2k hosts (/21)
255.255.240.0 - 4k hosts (/20)
255.255.224.0 - 8k hosts (/19)
255.255.192.0 - 16k hosts (/18)
255.255.128.0 - 32k hosts (/17)
255.255.0.0 - 64k hosts (/16)
255.254.0.0 - 128k hosts (/15)
255.252.0.0 - 256k hosts (/14)
255.248.0.0 - 512k hosts (/13)
255.240.0.0 - 1M hosts (/12)
255.224.0.0 - 2M hosts (/11)
255.192.0.0 - 4M hosts (/10)
255.128.0.0 - 8M hosts (/9)
255.0.0.0 - 16M hosts (/8)
254.0.0.0 - 32M hosts (/7)
252.0.0.0 - 64M hosts (/6)
248.0.0.0 - 128M hosts (/5)
240.0.0.0 - 256M hosts (/4)
224.0.0.0 - 512M hosts (/3)
192.0.0.0 - 1G hosts (/2)
128.0.0.0 - 2G hosts (/1)
0.0.0.0 - 4G hosts (/0)
Apply Cancel Help
Available interfaces
LAN
WAN (Static)
DMZ
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Edit settings of the WAN interface:
Change WAN Type: Static IP Apply Change
Static WAN interface configuration is most commonly used in dedicated-line internet connections.
Your ISP usually provides this information to you.
IP Address: 192.168.10.148
Subnet Mask: 255.255.255.0 - 256 hosts (/24)
Gateway IP: 192.168.10.254
Primary DNS Server: 192.168.10.249
Secondary DNS Server: (optional)
Manual MAC Address - change the hardware address of the interface
Some Internet service providers (ISPs) bind their service to a specific MAC address. In these cases you will have to change the MAC address of the firewall WAN interface. Input the address of the computer or network equipment that the service currently is bound to.
Warning! Do not change the hardware address unless the ISP requires it.
MAC Address:
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: 1500 bytes. Upper limit: 1500
Apply Cancel Help
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Edit settings of the WAN interface:
Change WAN Type: DHCP
Apply Change
Regular ethernet connection with DHCP-assigned IP addresses is used in many DSL and cable modem networks. Everything is automatic.
Manual MAC Address - change the hardware address of the interface
Some Internet service providers (ISPs) bind their service to a specific MAC address. In these cases you will have to change the MAC address of the firewall WAN interface. Input the address of the computer or network equipment that the service currently is bound to.
Warning! Do not change the hardware address unless the ISP requires it.
MAC Address:
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: 1500 bytes. Upper limit: 1500.
Apply Cancel Help
Available interfaces
LAN [Edit]
WAN (Static) [Edit]
DMZ [Edit]
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
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:
Password:
Retype Password:
Service Name:
(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: 192.168.10.249 (optional)
Secondary DNS Server: (optional)
Manual MAC Address - change the hardware address of the interface
Some Internet service providers (ISPs) bind their service to a specific MAC address. In these cases you will have to change the MAC address of the firewall WAN interface. Input the address of the computer or network equipment that the service currently is bound to.
Warning! Do not change the hardware address unless the ISP requires it.
MAC Address:
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.
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Edit settings of the WAN interface:
Change WAN Type: Big Pond Cable Apply Change
Regular ethernet connection with DHCP-assigned IP address, plus authentication via a special protocol. Used by the ISP Telstra BigPond (BigPond Broadband Cable) .
Username:
Password:
Retype Password:
Authenticaion server (optional):
Authenticaion domain (optional):
Authenticaion server port (optional): 5050
Leave authentication server settings blank to use default server, domain and port.
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: 1500 bytes. Upper limit: 1500.
Apply Cancel Help
Available interfaces
LAN [Edit]
WAN (Static) [Edit]
DMZ [Edit]
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Interface Settings
Edit settings of the DMZ interface:
IP Address: 127.0.0.1
Subnet Mask: 255.255.255.0 - 256 hosts (/24)
255.255.255.255 - 1 host (/32)
255.255.255.254 - 2 hosts (/31)
255.255.255.252 - 4 hosts (/30)
255.255.255.248 - 8 hosts (/29)
255.255.255.240 - 16 hosts (/28)
255.255.255.224 - 32 hosts (/27)
255.255.255.192 - 64 hosts (/26)
255.255.255.128 - 128 hosts (/25)
255.255.255.0 - 256 hosts (/24)
255.255.254.0 - 512 hosts (/23)
255.255.252.0 - 1k hosts (/22)
255.255.248.0 - 2k hosts (/21)
255.255.240.0 - 4k hosts (/20)
255.255.224.0 - 8k hosts (/19)
255.255.192.0 - 16k hosts (/18)
255.255.128.0 - 32k hosts (/17)
255.255.0.0 - 64k hosts (/16)
255.254.0.0 - 128k hosts (/15)
255.252.0.0 - 256k hosts (/14)
255.248.0.0 - 512k hosts (/13)
255.240.0.0 - 1M hosts (/12)
255.224.0.0 - 2M hosts (/11)
255.192.0.0 - 4M hosts (/10)
255.128.0.0 - 8M hosts (/9)
255.0.0.0 - 16M hosts (/8)
254.0.0.0 - 32M hosts (/7)
252.0.0.0 - 64M hosts (/6)
248.0.0.0 - 128M hosts (/5)
240.0.0.0 - 256M hosts (/4)
224.0.0.0 - 512M hosts (/3)
Apply Cancel Help
Available interfaces
LAN
WAN (Static)
DMZ
Internet

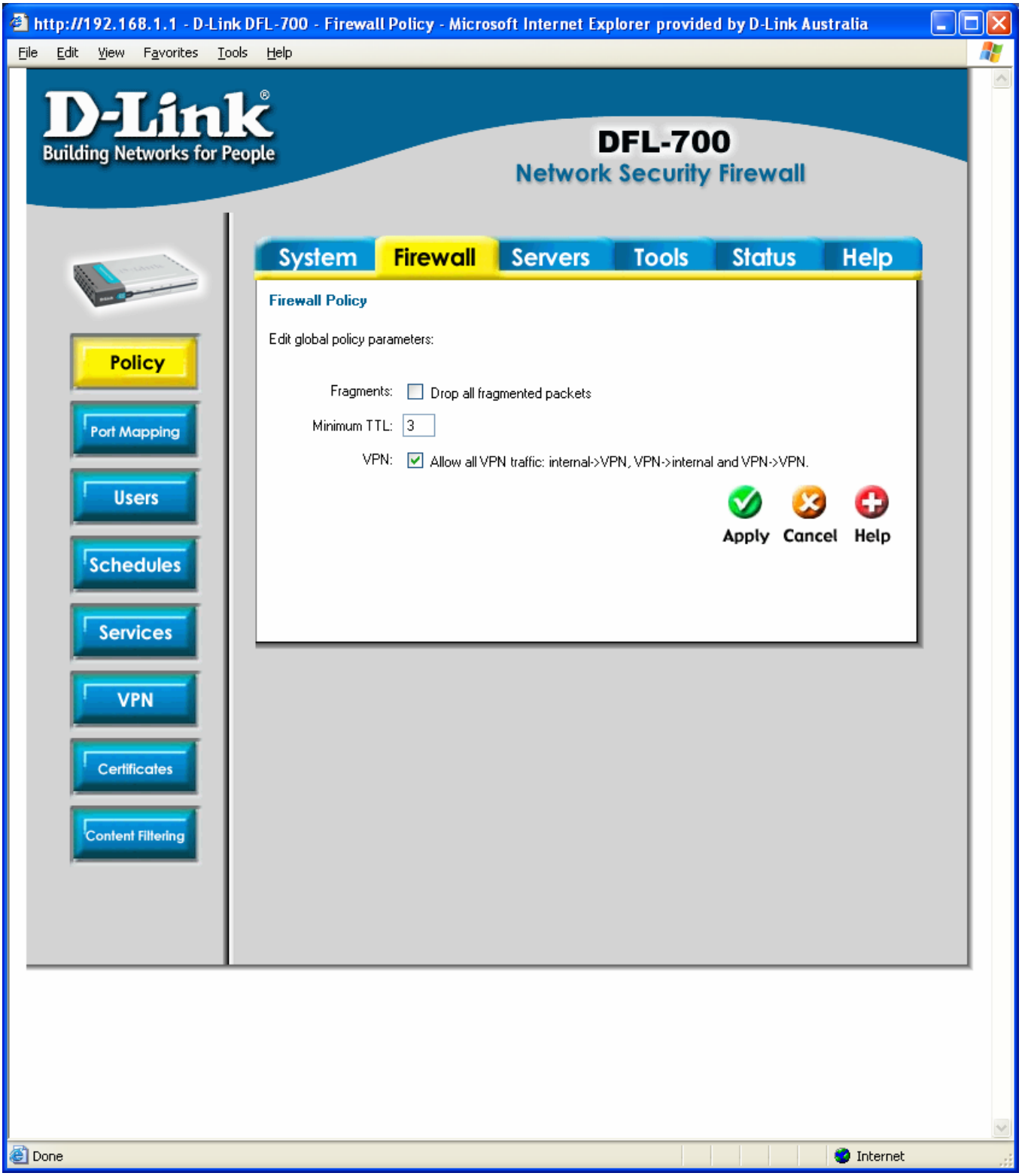

http://192.168.1.1 - D-Link DFL-700 - Routing Table - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Administration
Interfaces
Routing
Logging
Time
System Firewall Servers Tools Status 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 192.168.10.0/24 [Edit]
WAN 0.0.0.0/0 192.168.10.254 [Edit]
DMZ 127.0.0.0/24 [Edit]
[Add new]
Internet


http://192.168.1.1 - D-Link DFL-700 - Routing Table - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Routing Table
Edit new route:
Interface: LAN
Network:
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 192.168.10.0/24 [Edit]
WAN 0.0.0.0/0 192.168.10.254 [Edit]
DMZ 127.0.0.0/24 [Edit]
[Add new]
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Logging Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
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: 192.168.1.2
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
Done
Internet

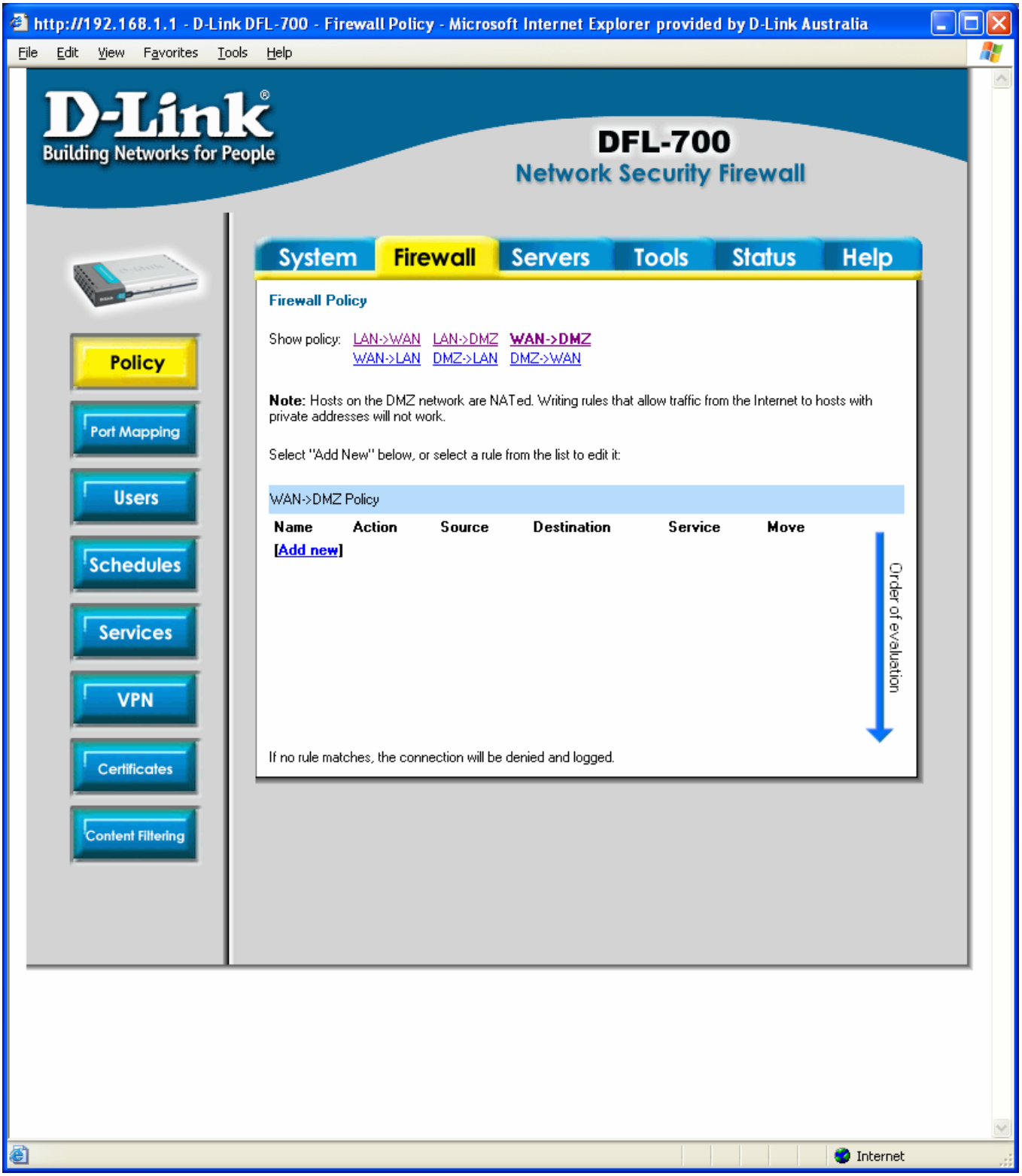

http://192.168.1.1 - D-Link DFL-700 - Time Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Administration
Interfaces
Routing
Logging
Time
Time Settings
Current time and date
Set the system time
Date: 21 Dec 2006
Time: 23:56:46 (24 hour time)
Time zone and daylight saving time settings
Time zone: (GMT) Dublin, Edinburgh, Lisbon, London, Casablanca, Monrovia
No daylight saving time
Apply daylight saving time from: Jan 01
... to: Jan 01
Automatic time synchronization
Enable NTP
Primary NTP Server:
Secondary NTP Server: (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
Internet

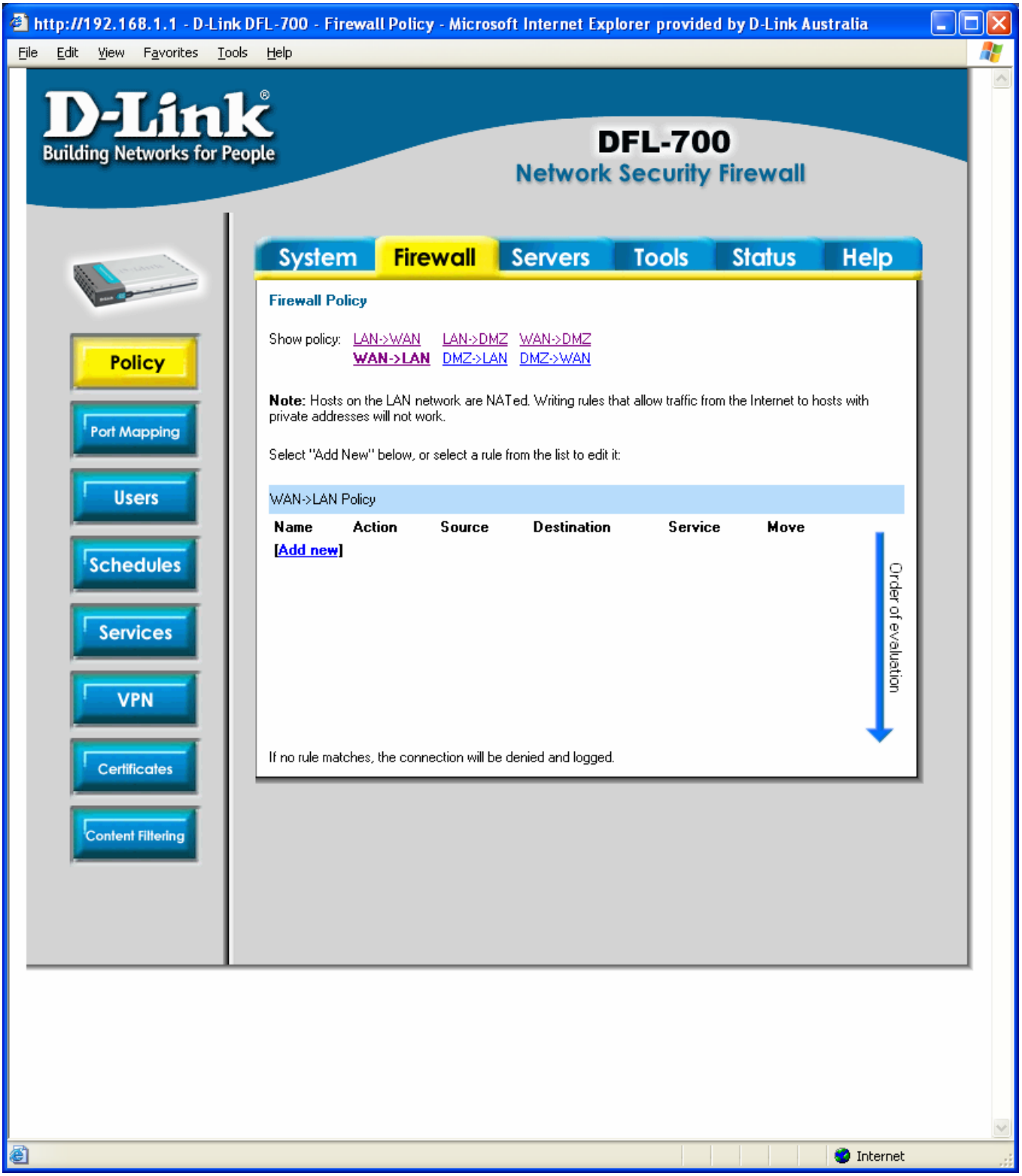

http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
System
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
Internet

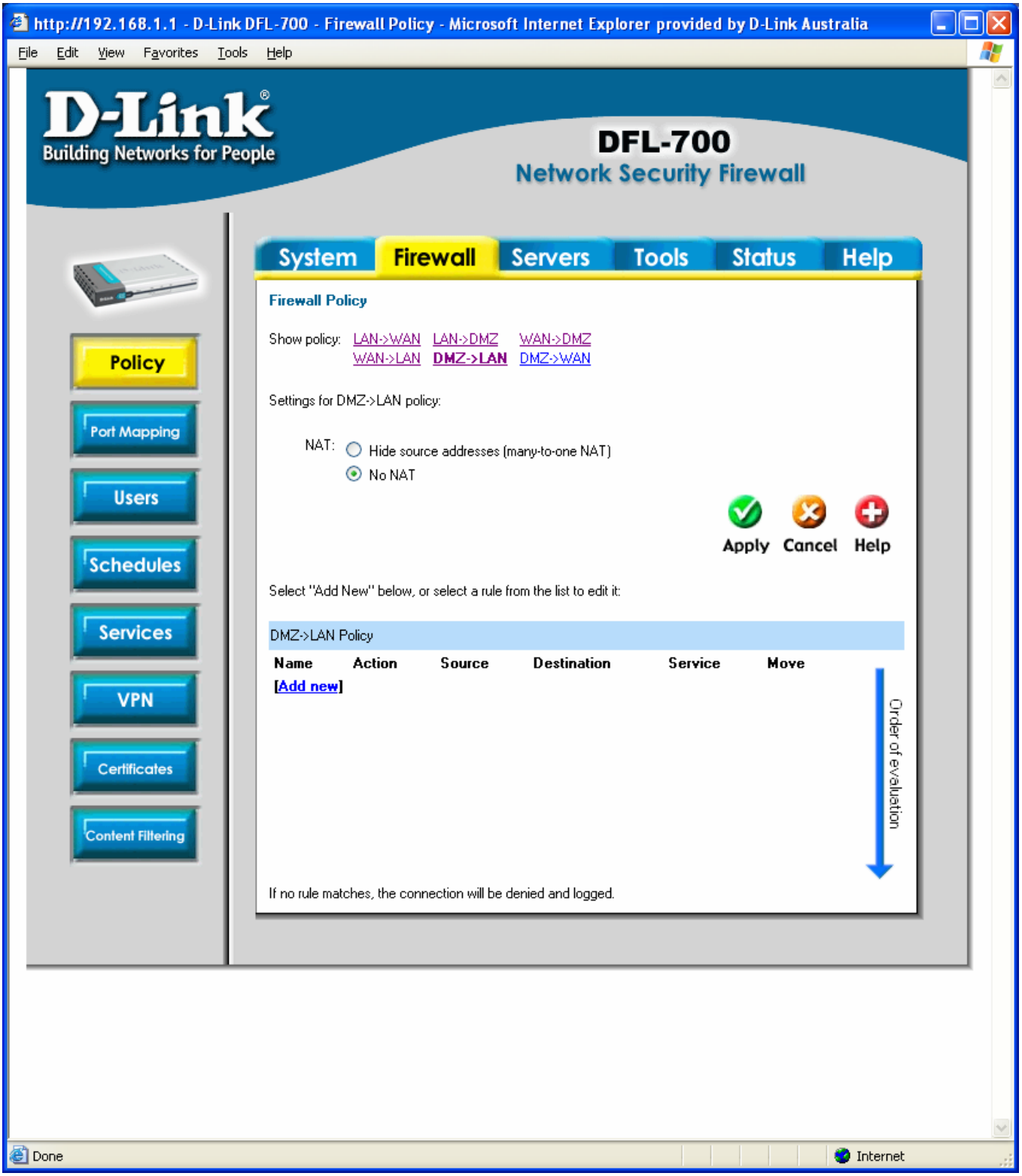

http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Firewall
Servers
Tools
Status
Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
Firewall Policy
Edit global policy parameters:
Fragments:
Drop all fragmented packets
Minimum TTL:
3
VPN:
Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.
Apply
Cancel
Help
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
WAN->LAN DMZ->LAN DMZ->WAN
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 Move
#1 drop_smb-all Allow 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.
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
Firewall Policy
Show policy: LAN->WAN LAN->DMZ WAN->DMZ WAN->LAN DMZ->LAN DMZ->WAN
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 Move
#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.
Internet


http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
WAN->LAN DMZ->LAN DMZ->WAN
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 Move
[Add new]
Order of evaluation
If no rule matches, the connection will be denied and logged.
Internet


http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
WAN->LAN DMZ->LAN DMZ->WAN
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 Move
[Add new]
Order of evaluation
If no rule matches, the connection will be denied and logged.
Internet


http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
WAN->LAN DMZ->LAN DMZ->WAN
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 Move
[Add new]
Order of evaluation
If no rule matches, the connection will be denied and logged.
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Firewall Policy - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
WAN->LAN DMZ->LAN DMZ->WAN
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 Move
#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.
Done
Internet

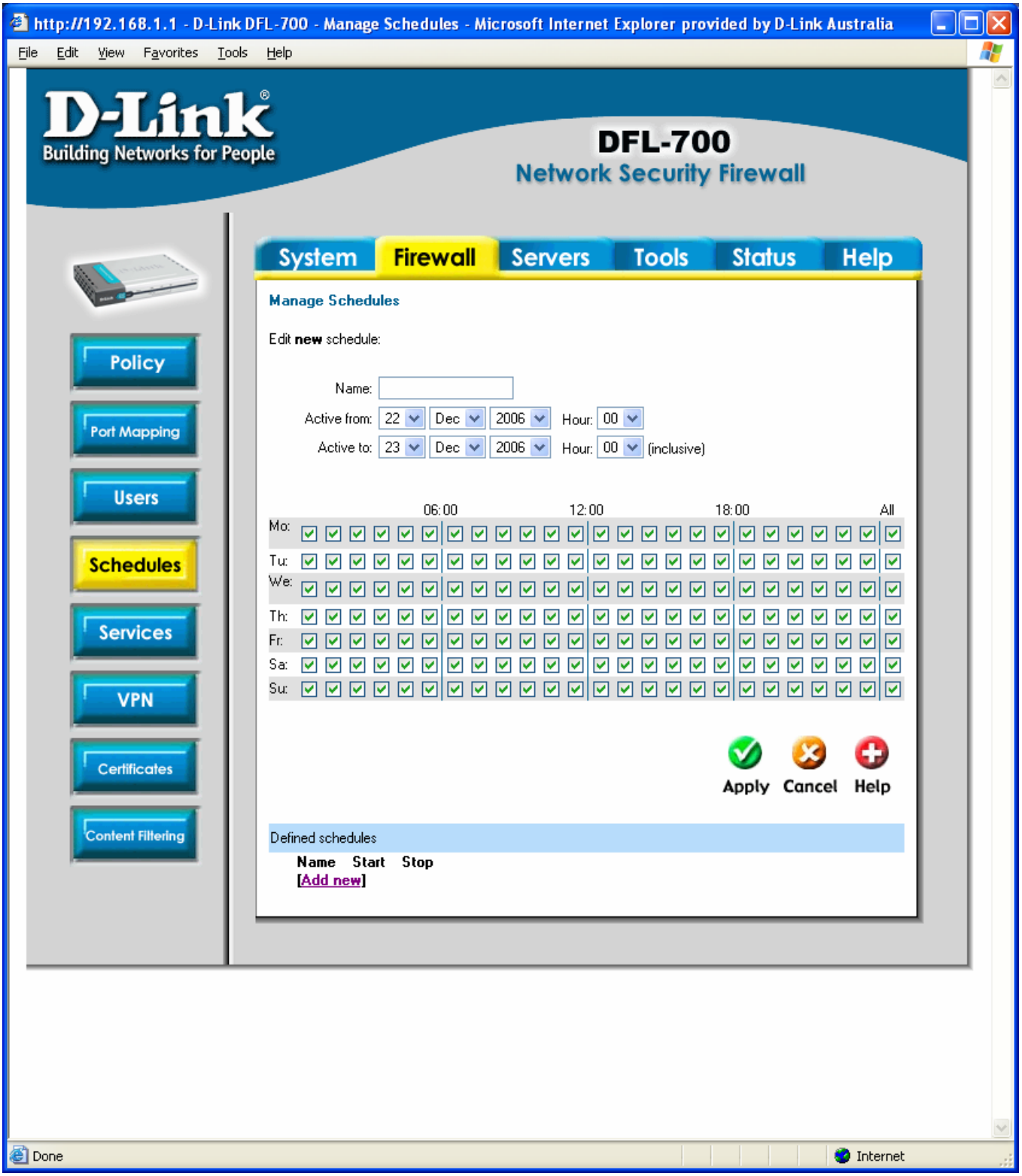

http://192.168.1.1 - D-Link DFL-700 - Port Mapping / Virtual Servers - Microsoft Internet Explorer provided by D-Lin...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
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]
Internet


http://192.168.1.1 - D-Link DFL-700 - Port Mapping / Virtual Servers - Microsoft Internet Explorer provided by D-Lin...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - User Management - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
User Management
Enable User Authentication via HTTP / HTTPS
HTTP Security: HTTP as well as HTTPS
HTTPS only
Idle Timeout: 2 hours
Authentication source:
Local database
RADIUS server
Primary Server: port 1812
Secondary Server: port 1812
Mode: PAP
Shared Secret:
Retype Secret:
RADIUS retry: 2 seconds
Note: Administration of this unit can only be made by administrative users in the local database.
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 Client IP
[Add new]
Internet

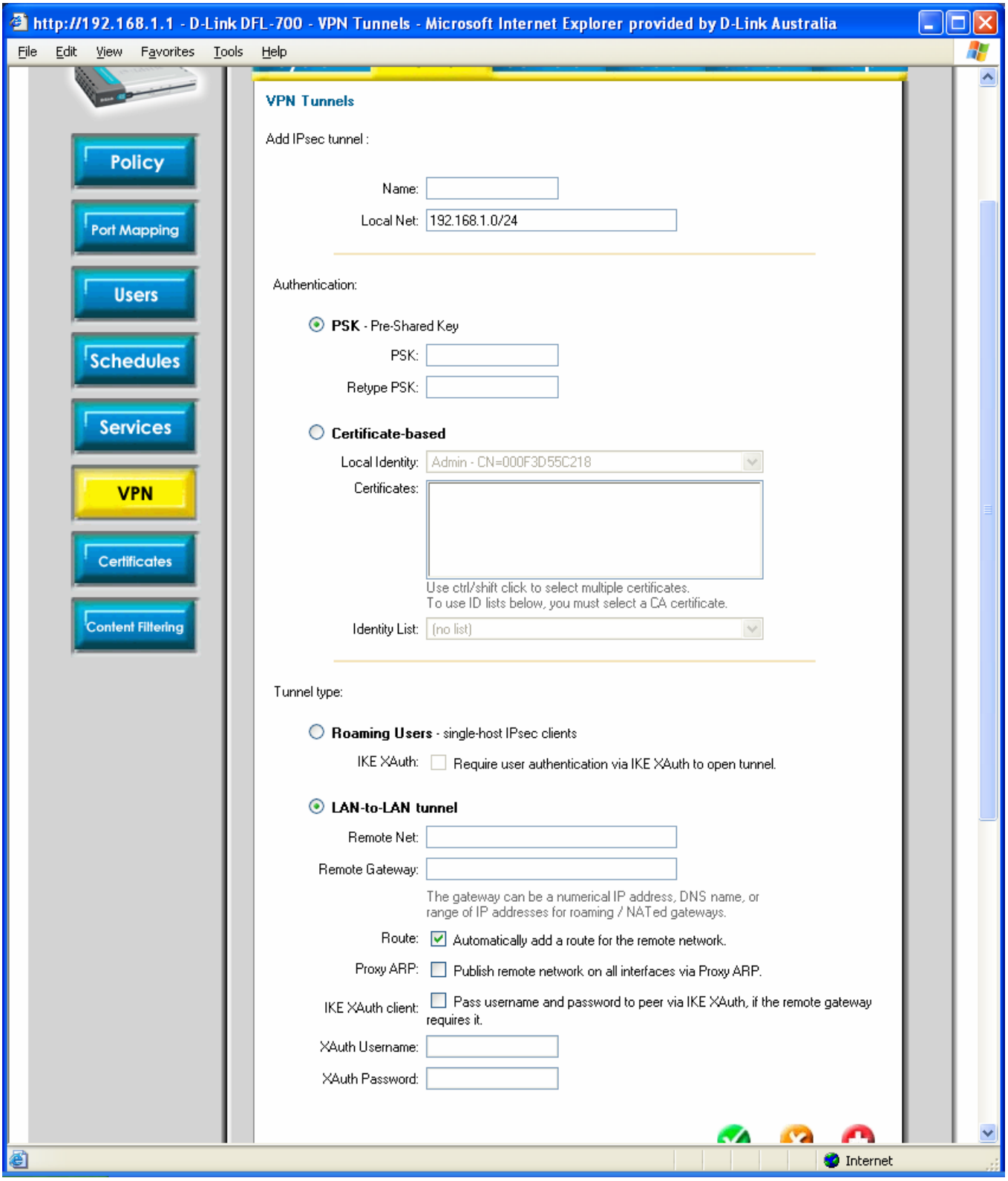

http://192.168.1.1 - D-Link DFL-700 - User Management - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
System Firewall Servers Tools Status Help
User Management
Add new user:
User name:
Group membership:
Password:
Retype password:
L2TP/PPTP settings:
Static client IP:
If empty, the IP address will be taken from the server's IP pool
Networks behind user:
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 Client IP
[Add new]
Done
Internet

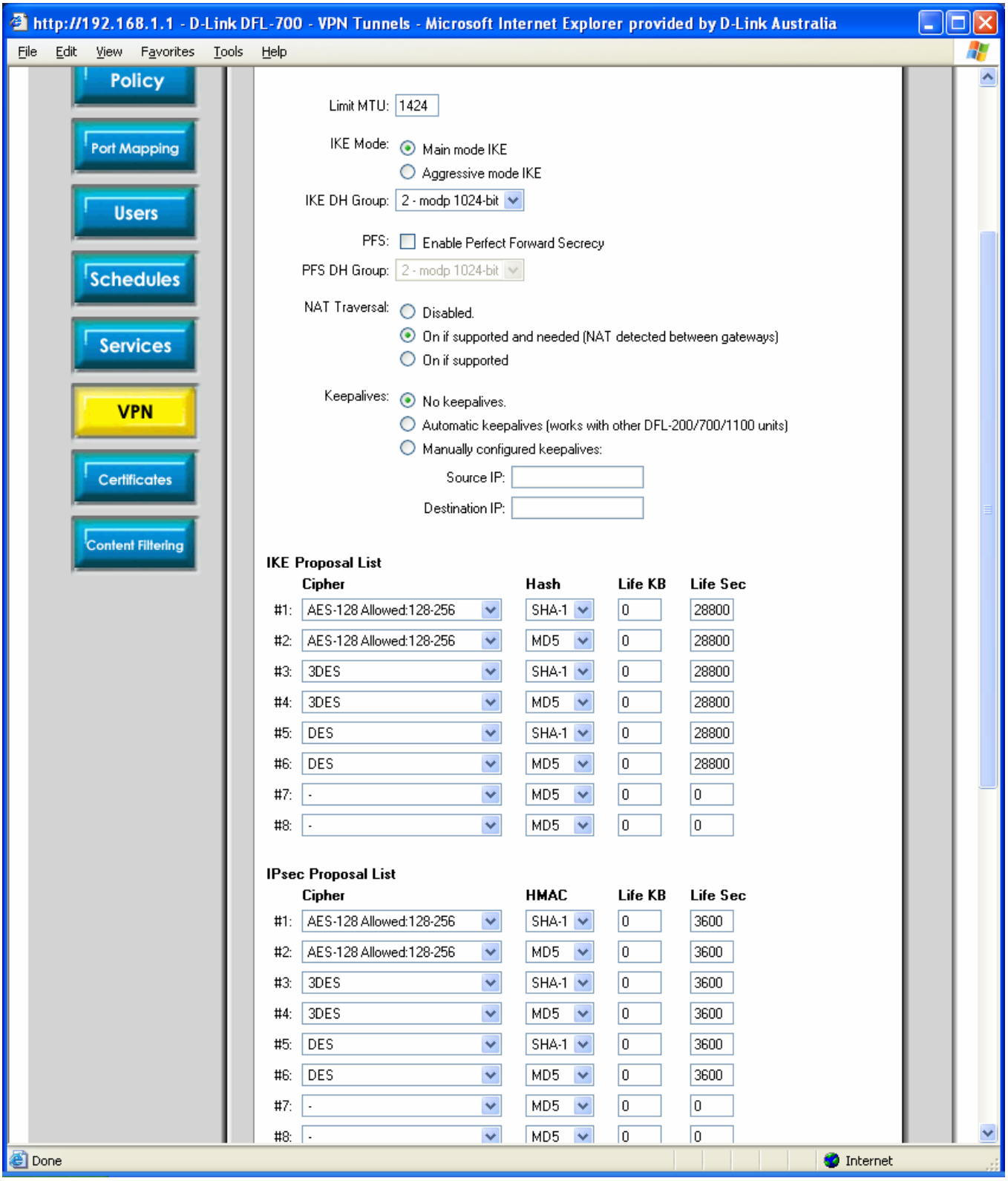

http://192.168.1.1 - D-Link DFL-700 - Manage Schedules - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Firewall
Servers
Tools
Status
Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
Manage Schedules
Pick a schedule to edit from the below list:
Help
Available schedules
Name Start Stop
[Add new]
Done
Internet

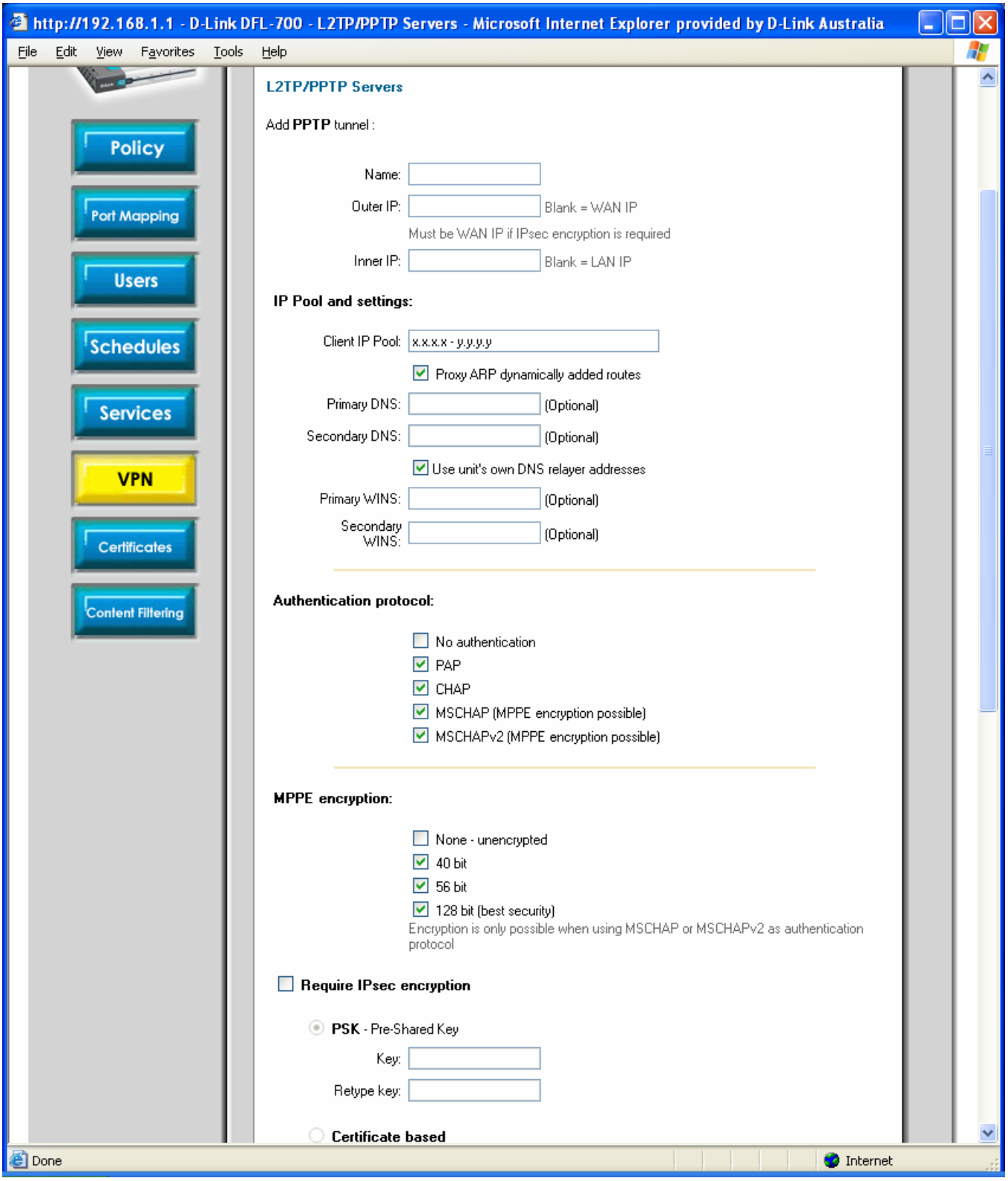

http://192.168.1.1 - D-Link DFL-700 - Manage Schedules - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
Manage Schedules
Edit new schedule:
Name:
Active from: 22 Dec 2006 Hour: 00
Active to: 23 Dec 2006 Hour: 00 (inclusive)
06:00 12:00 18:00 All
Mo:
Tu:
We:
Th:
Fr:
Sa:
Su:
Apply Cancel Help
Defined schedules
Name Start Stop
[Add new]
Done
Internet

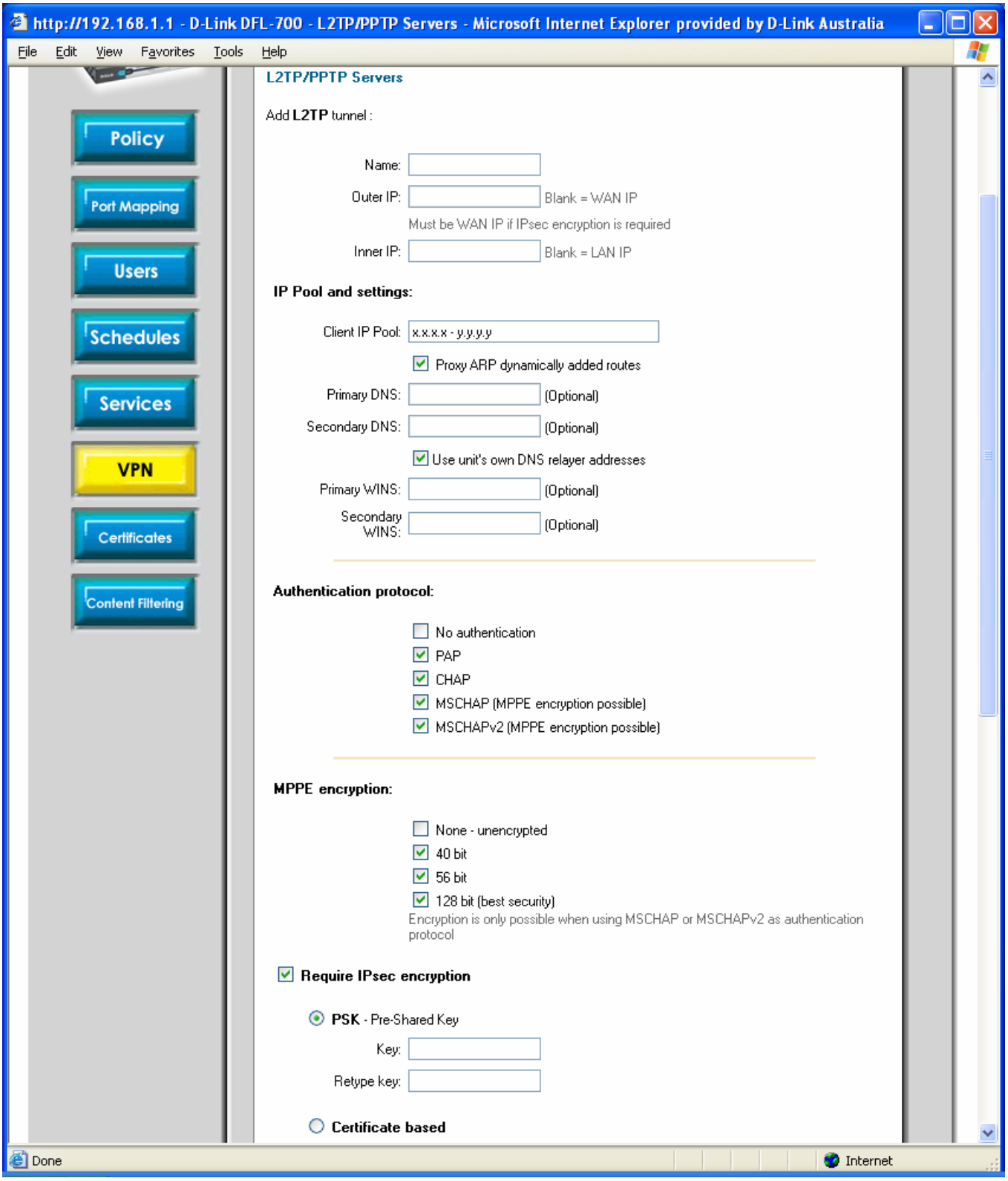

http://192.168.1.1 - D-Link DFL-700 - Services Settings - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
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]
Internet

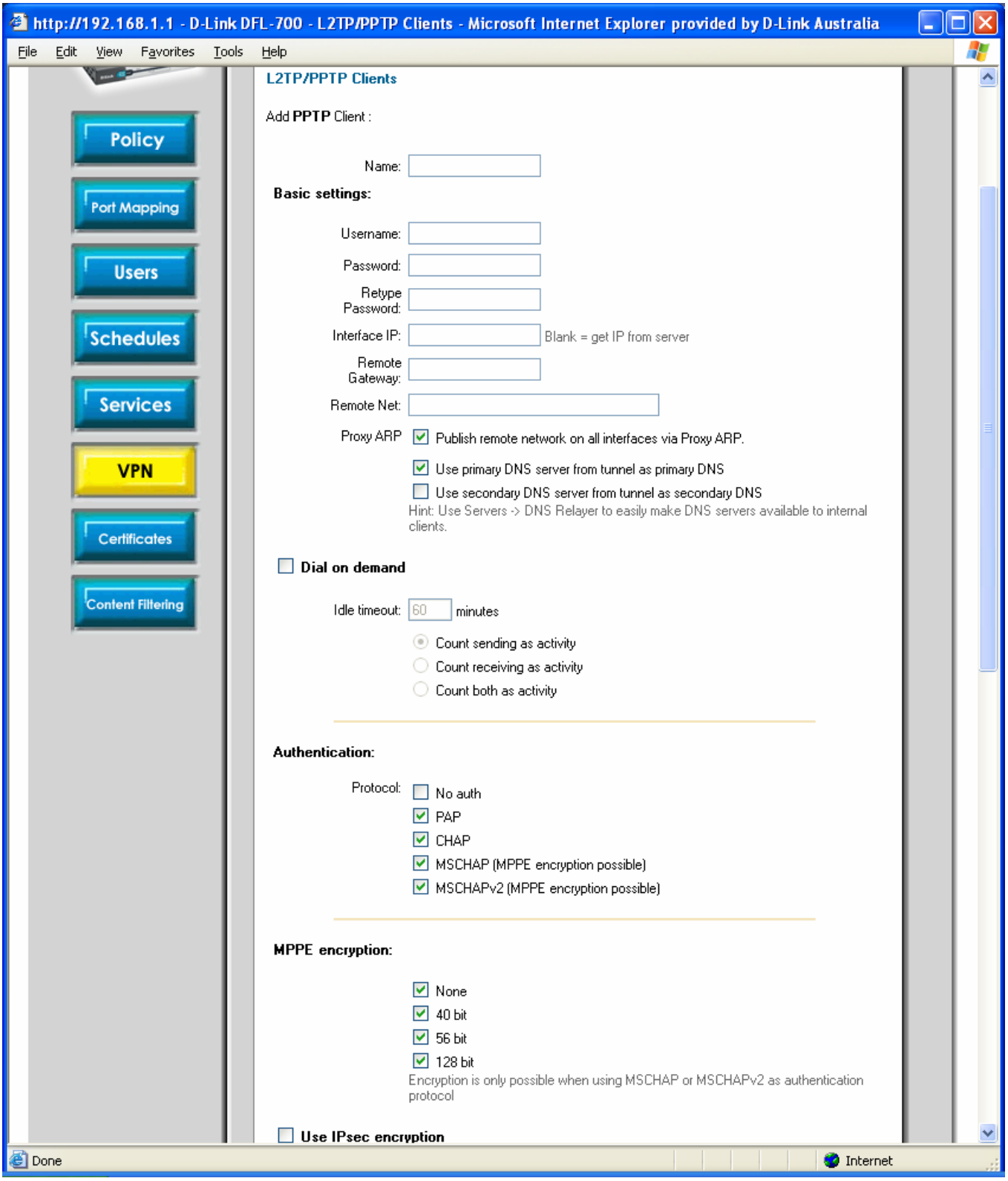

http://192.168.1.1 - D-Link DFL-700 - VPN Tunnels - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
System Firewall Servers Tools Status Help
VPN Tunnels
Pick a VPN tunnel to edit from the below list:
Help
IPsec Tunnels
Name Local Net Remote Net Remote Gateway
[Add new]
L2TP / PPTP Client
Name Type Remote Gateway User IPsec
[Add new PPTP client]
[Add new L2TP client]
L2TP / PPTP Server
Name Type Outer IP Inner IP IPsec
[Add new PPTP server]
[Add new L2TP server]
Internet

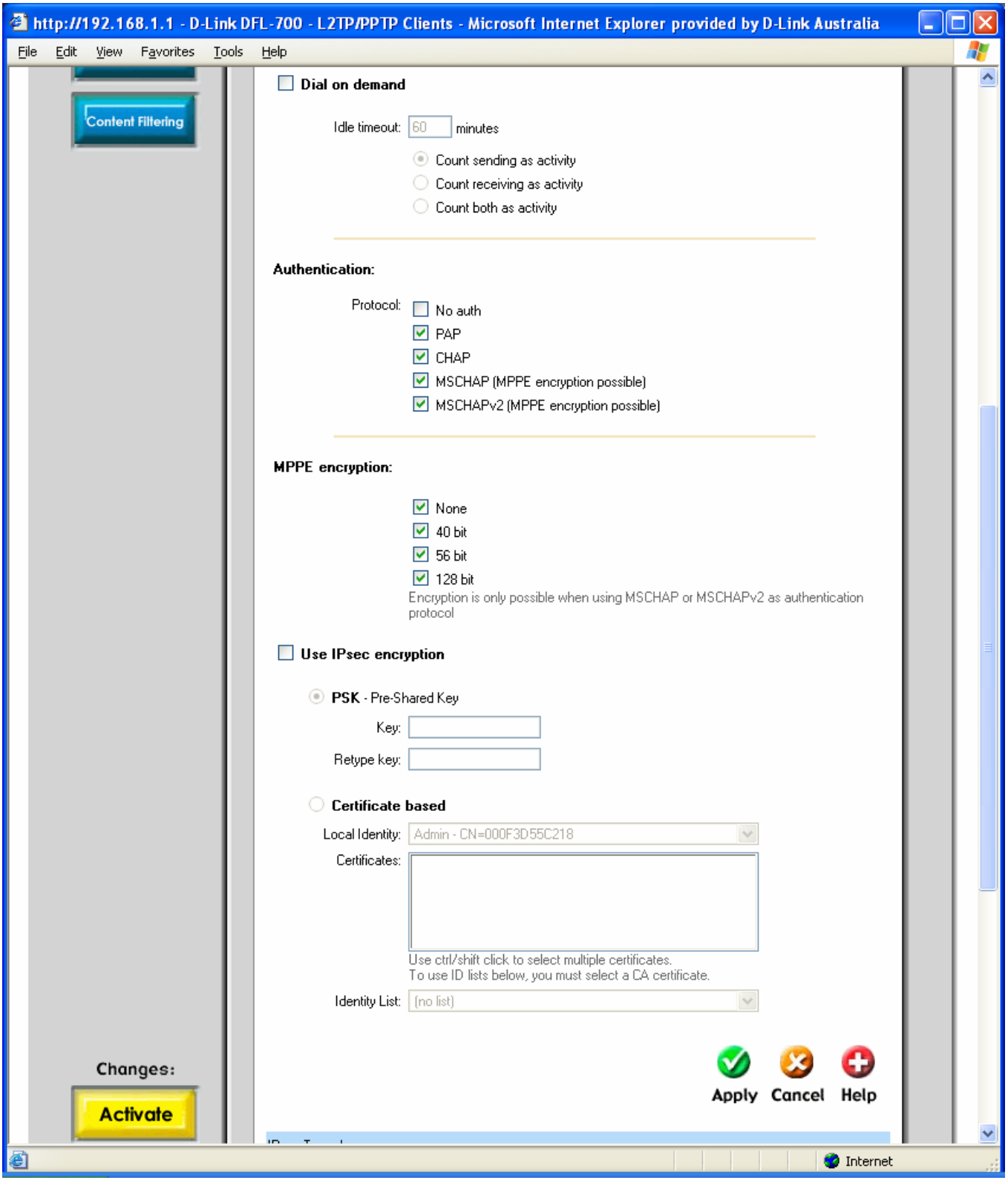

http://192.168.1.1 - D-Link DFL-700 - VPN Tunnels - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
VPN Tunnels
Add IPsec tunnel :
Name:
Local Net: 192.168.1.0/24
Authentication:
PSK - Pre-Shared Key
PSK:
Retype PSK:
Certificate-based
Local Identity: Admin - CN=000F3D55C218
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 IPsec 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.
Route: Automatically add a route for the remote network.
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:
Internet


http://192.168.1.1 - D-Link DFL-700 - VPN Tunnels - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
Limit MTU: 1424
IKE Mode: Main mode IKE
Aggressive mode IKE
IKE DH Group: 2 - modp 1024-bit
PFS: Enable Perfect Forward Secrecy
PFS DH Group: 2 - modp 1024-bit
NAT Traversal: Disabled.
On if supported and needed (NAT detected between gateways)
On if supported
Keepalives: No keepalives.
Automatic keepalives (works with other DFL-200/700/1100 units)
Manually configured keepalives:
Source IP:
Destination IP:
IKE Proposal List
Cipher Hash Life KB Life Sec
#1: AES-128 Allowed:128-256 SHA-1 0 28800
#2: AES-128 Allowed:128-256 MD5 0 28800
#3: 3DES SHA-1 0 28800
#4: 3DES MD5 0 28800
#5: DES SHA-1 0 28800
#6: DES MD5 0 28800
#7: - MD5 0 0
#8: - MD5 0 0
IPsec Proposal List
Cipher HMAC Life KB Life Sec
#1: AES-128 Allowed:128-256 SHA-1 0 3600
#2: AES-128 Allowed:128-256 MD5 0 3600
#3: 3DES SHA-1 0 3600
#4: 3DES MD5 0 3600
#5: DES SHA-1 0 3600
#6: DES MD5 0 3600
#7: - MD5 0 0
#8: - MD5 0 0
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - L2TP/PPTP Servers - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
L2TP/PPTP Servers
Add PPTP tunnel :
Name:
Outer IP: Blank = WAN IP
Must be WAN IP if IPsec encryption is required
Inner IP: Blank = LAN IP
IP Pool and settings:
Client IP Pool: x.x.x.x - y.y.y.y
Proxy ARP dynamically added routes
Primary DNS: (Optional)
Secondary DNS: (Optional)
Use unit's own DNS relayer addresses
Primary WINS: (Optional)
Secondary WINS: (Optional)
Authentication protocol:
No authentication
PAP
CHAP
MSCHAP (MPPE encryption possible)
MSCHAPv2 (MPPE encryption possible)
MPPE encryption:
None - unencrypted
40 bit
56 bit
128 bit (best security)
Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol
Require IPsec encryption
PSK - Pre-Shared Key
Key:
Retype key:
Certificate based
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - L2TP/PPTP Servers - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
L2TP/PPTP Servers
Add L2TP tunnel :
Name:
Outer IP:
Blank = WAN IP
Must be WAN IP if IPsec encryption is required
Inner IP:
Blank = LAN IP
IP Pool and settings:
Client IP Pool:
x.x.x.x - y.y.y.y
Proxy ARP dynamically added routes
Primary DNS:
(Optional)
Secondary DNS:
(Optional)
Use unit's own DNS relayer addresses
Primary WINS:
(Optional)
Secondary WINS:
(Optional)
Authentication protocol:
No authentication
PAP
CHAP
MSCHAP (MPPE encryption possible)
MSCHAPv2 (MPPE encryption possible)
MPPE encryption:
None - unencrypted
40 bit
56 bit
128 bit (best security)
Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol
Require IPsec encryption
PSK - Pre-Shared Key
Key:
Retype key:
Certificate based
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - L2TP/PPTP Clients - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
L2TP/PPTP Clients
Add PPTP Client :
Name:
Basic settings:
Username:
Password:
Retype Password:
Interface IP:
Blank = get IP from server
Remote Gateway:
Remote Net:
Proxy ARP
Publish remote network on all interfaces via Proxy ARP.
Use primary DNS server from tunnel as primary DNS
Use secondary DNS server from tunnel as secondary DNS
Hint: Use Servers -> DNS Relayer to easily make DNS servers available to internal clients.
Dial on demand
Idle timeout: 60 minutes
Count sending as activity
Count receiving as activity
Count both as activity
Authentication:
Protocol:
No auth
PAP
CHAP
MSCHAP (MPPE encryption possible)
MSCHAPv2 (MPPE encryption possible)
MPPE encryption:
None
40 bit
56 bit
128 bit
Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol
Use IPsec encryption
Done
Internet

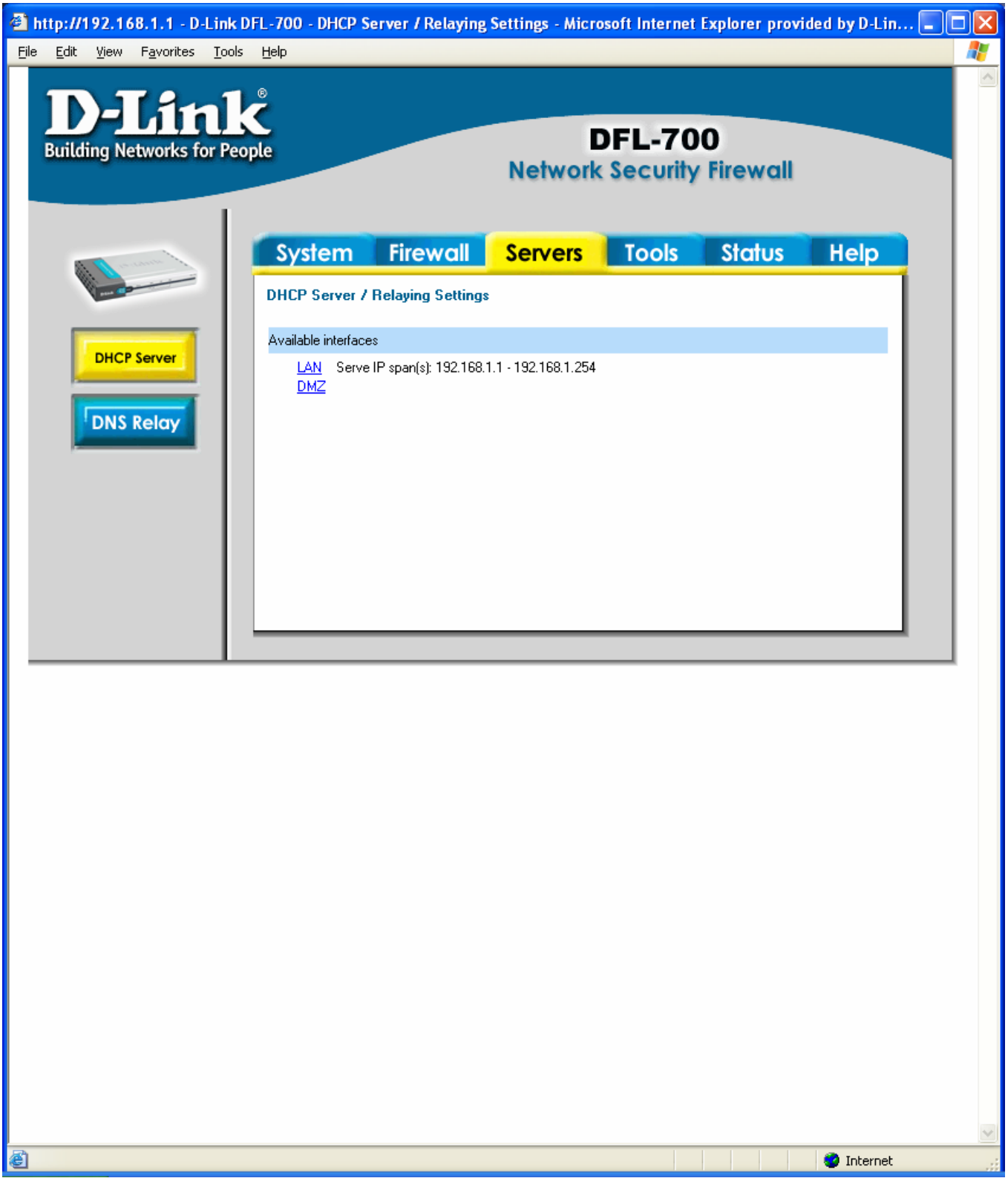

http://192.168.1.1 - D-Link DFL-700 - L2TP/PPTP Clients - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Content Filtering
Dial on demand
Idle timeout: 60 minutes
Count sending as activity
Count receiving as activity
Count both as activity
Authentication:
Protocol:
No auth
PAP
CHAP
MSCHAP (MPPE encryption possible)
MSCHAPv2 (MPPE encryption possible)
MPPE encryption:
None
40 bit
56 bit
128 bit
Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol
Use IPsec encryption
PSK - Pre-Shared Key
Key:
Retype key:
Certificate based
Local Identity: Admin - CN=000F3D55C218
Certificates:
Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.
Identity List: (no list)
Apply
Cancel
Help
Changes:
Activate
Internet

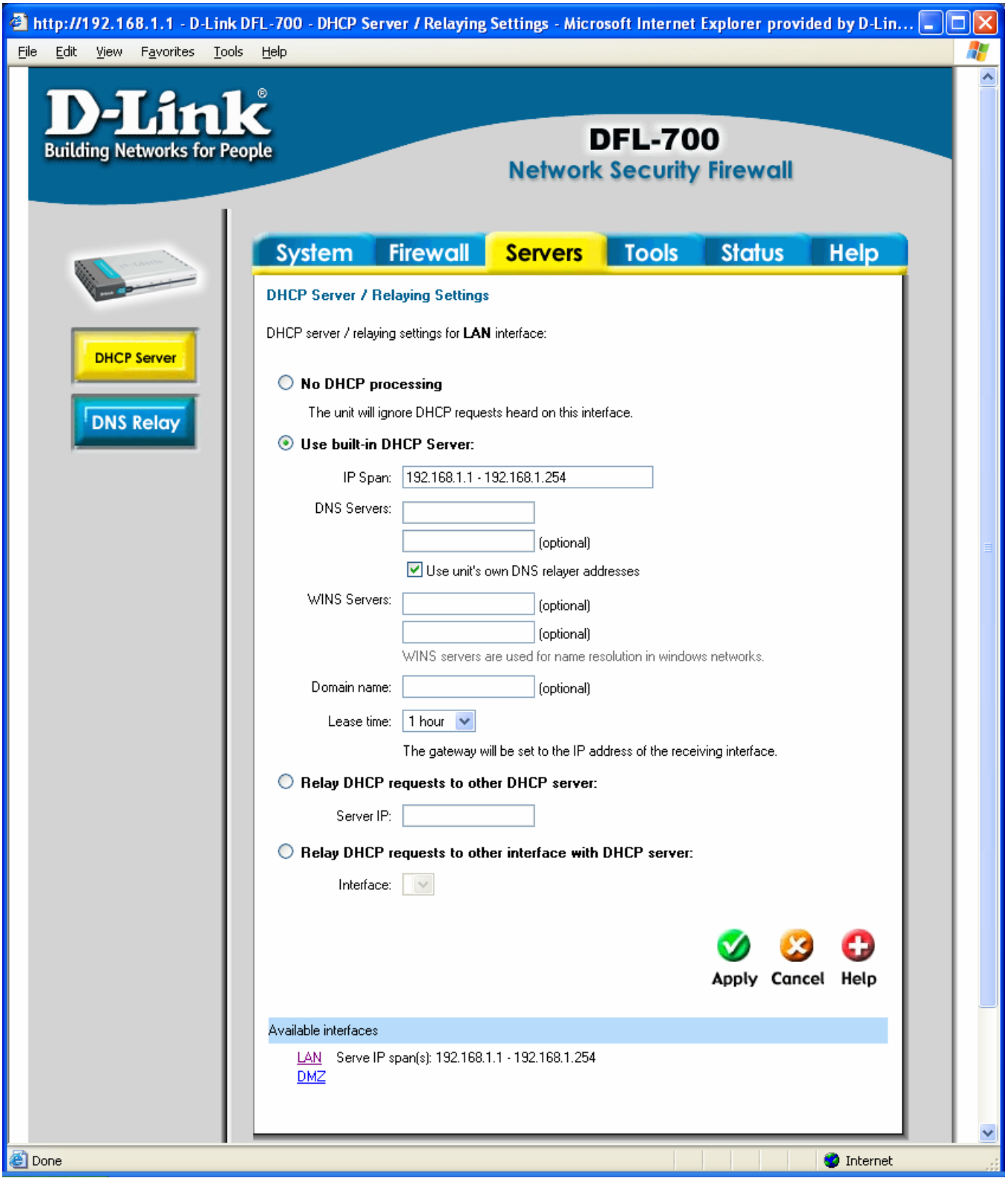

http://192.168.1.1 - D-Link DFL-700 - Manage Certificates - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Firewall
Servers
Tools
Status
Help
Policy
Port Mapping
Users
Schedules
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=000F3D55C218 2032-01-20 CN=000F3D55C218 [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]
Internet

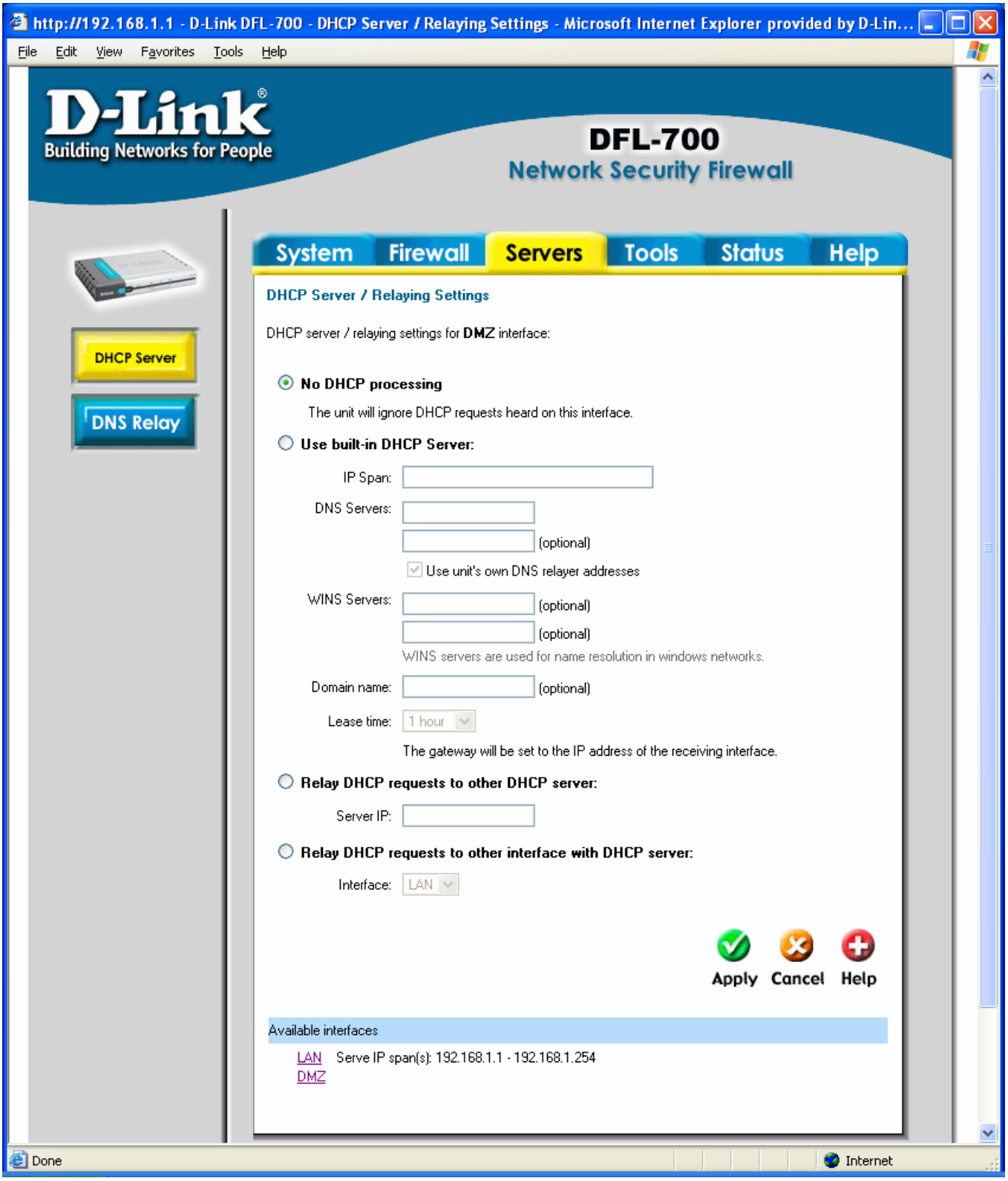

http://192.168.1.1 - D-Link DFL-700 - HTTP Content Filtering - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Firewall
Servers
Tools
Status
Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
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
Block Invalid Formatted UTF-8 Characters
Warning:
None of the policy rules use a service with the "HTTP/HTML Content Filtering" ALG!
Apply
Cancel
Help
Internet


http://192.168.1.1 - D-Link DFL-700 - HTTP Content Filtering - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
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
Done
Internet

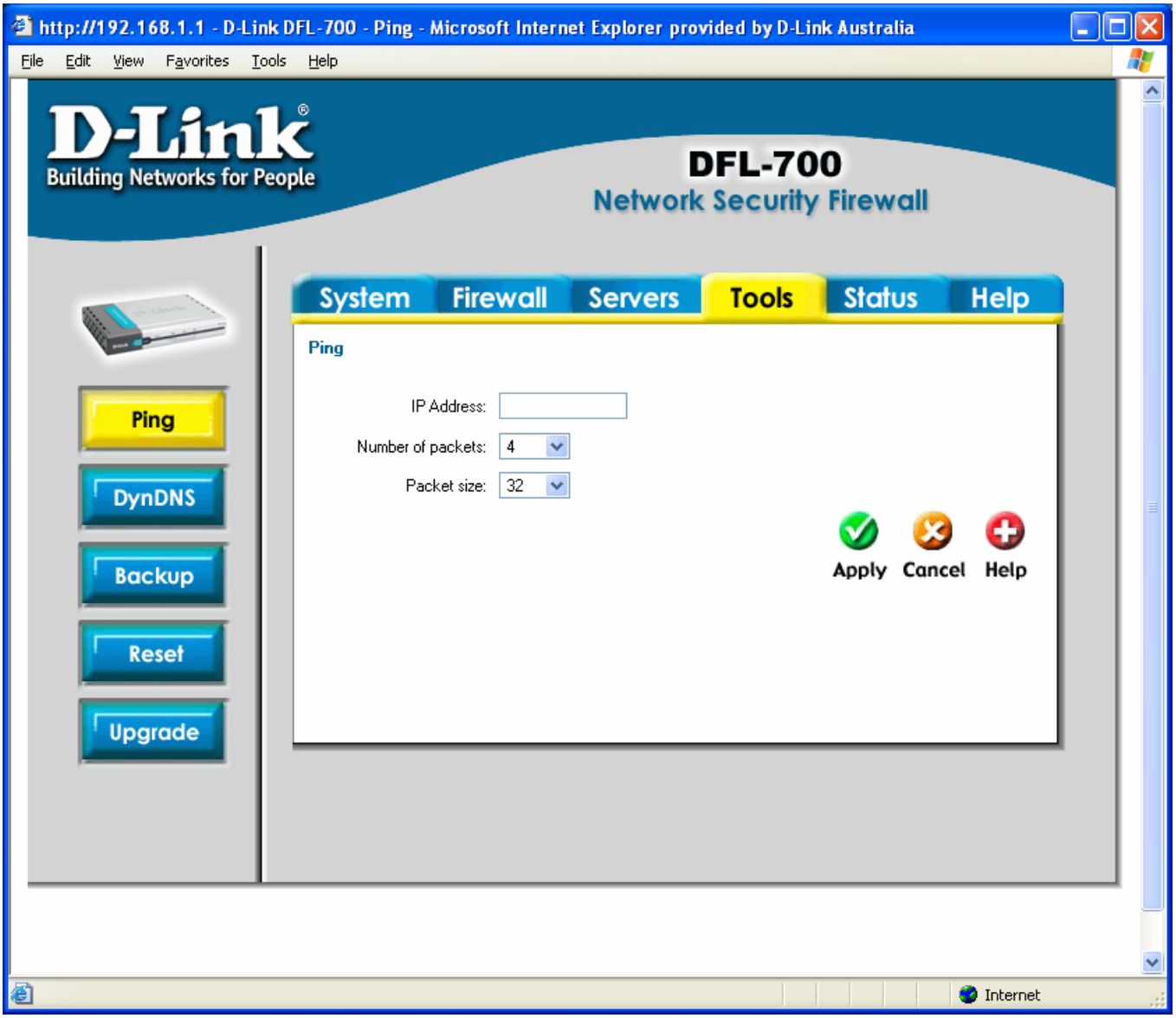

http://192.168.1.1 - D-Link DFL-700 - HTTP Content Filtering - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Policy
Port Mapping
Users
Schedules
Services
VPN
Certificates
Content Filtering
HTTP Content Filtering
Edit Destination URL Global 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
Done
Internet

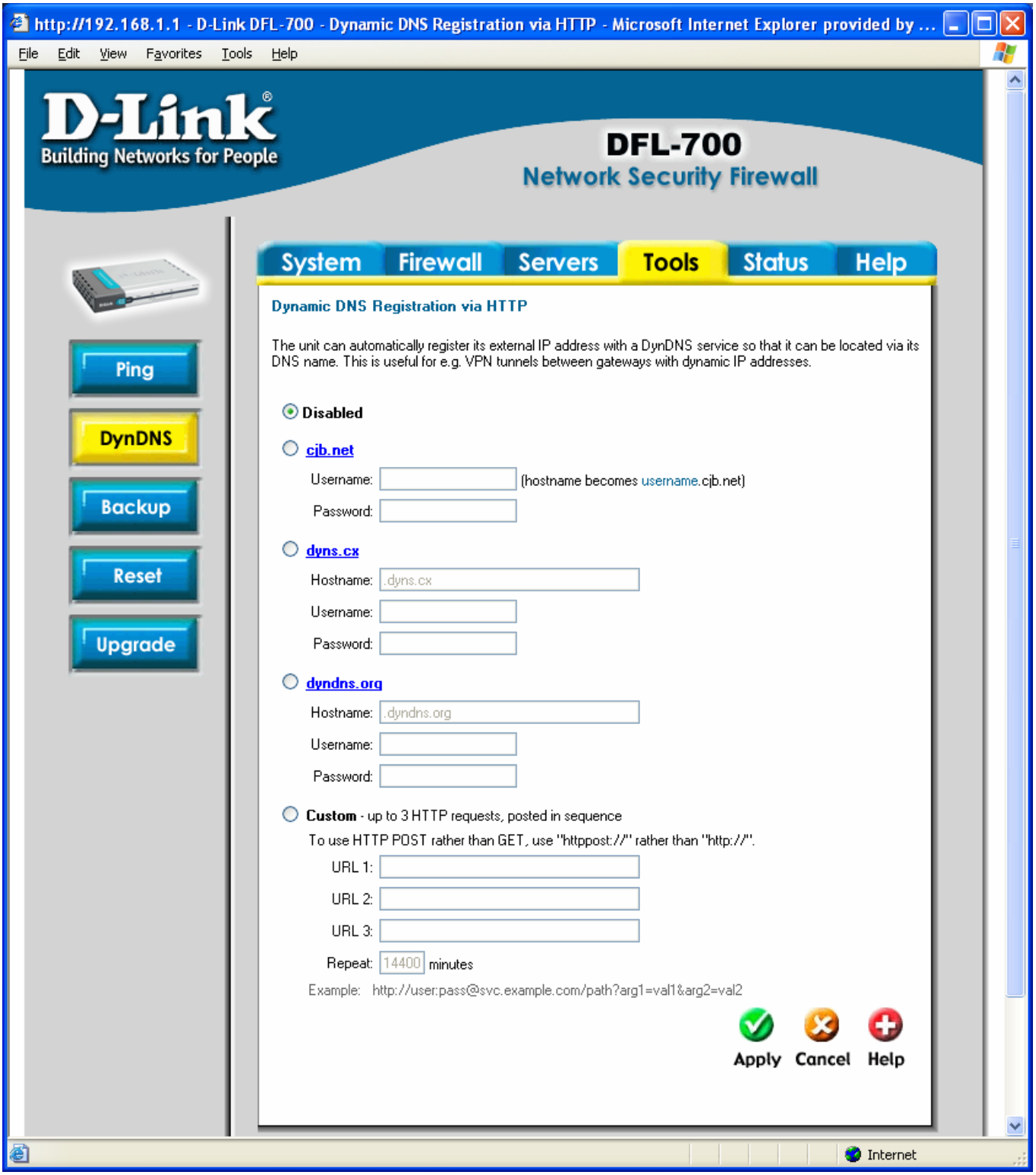

http://192.168.1.1 - D-Link DFL-700 - DHCP Server / Relaying Settings - Microsoft Internet Explorer provided by D-Lin...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
DHCP Server
DNS Relay
DHCP Server / Relaying Settings
Available interfaces
LAN Serve IP span(s): 192.168.1.1 - 192.168.1.254
DMZ
Internet

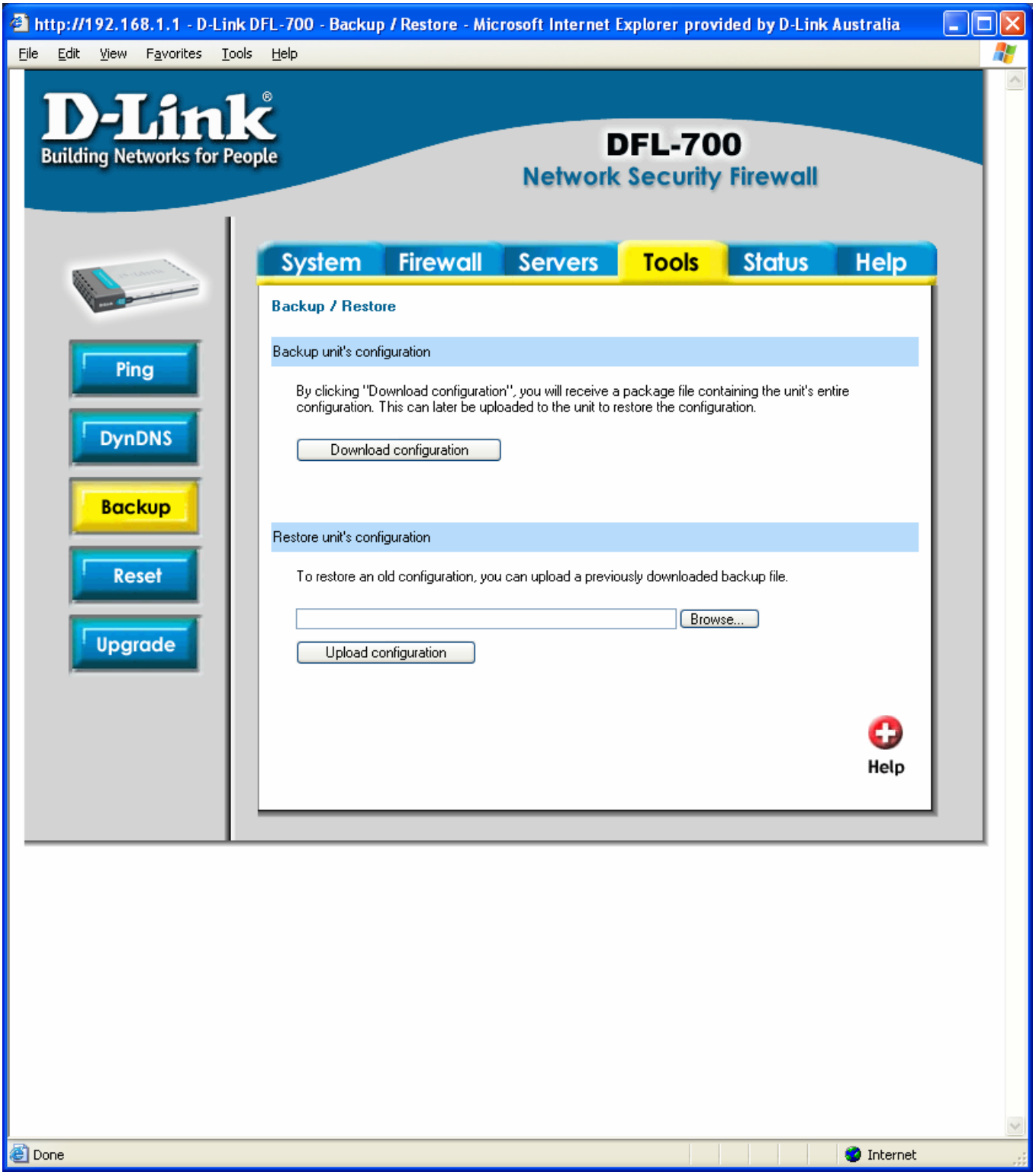

http://192.168.1.1 - D-Link DFL-700 - DHCP Server / Relaying Settings - Microsoft Internet Explorer provided by D-Lin...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
DHCP Server
DNS Relay
System Firewall Servers Tools Status Help
DHCP Server / 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: 192.168.1.1 - 192.168.1.254
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:
Relay DHCP requests to other interface with DHCP server:
Interface:
Apply Cancel Help
Available interfaces
LAN Serve IP span(s): 192.168.1.1 - 192.168.1.254
DMZ
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - DHCP Server / Relaying Settings - Microsoft Internet Explorer provided by D-Lin...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
DHCP Server
DNS Relay
System Firewall Servers Tools Status Help
DHCP Server / Relaying Settings
DHCP server / relaying settings for DMZ 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:
Relay DHCP requests to other interface with DHCP server:
Interface:
LAN
Apply
Cancel
Help
Available interfaces
LAN Serve IP span(s): 192.168.1.1 - 192.168.1.254
DMZ
Done
Internet

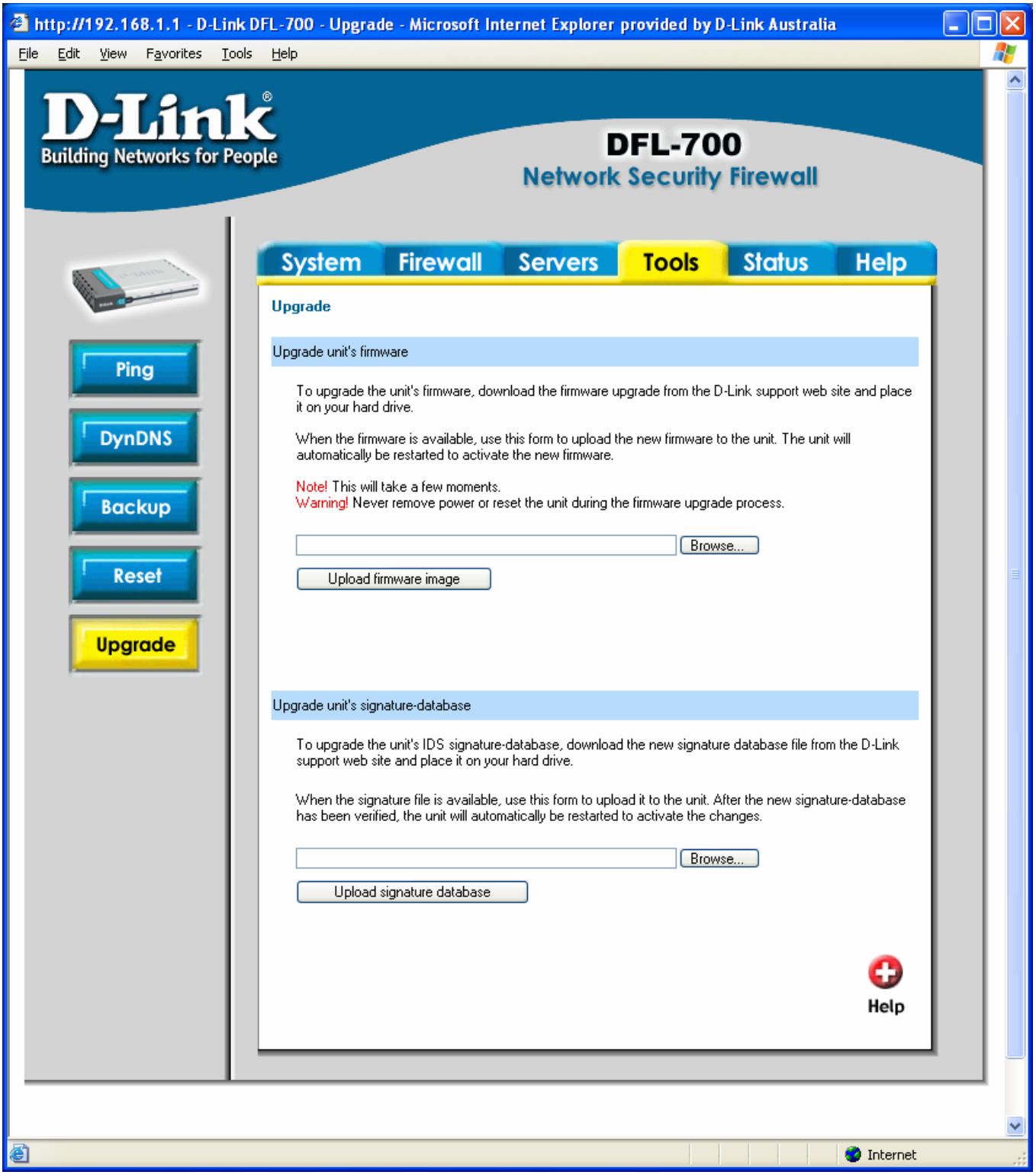

http://192.168.1.1 - D-Link DFL-700 - DNS Relay - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
DHCP Server
DNS Relay
System Firewall Servers Tools Status Help
DNS Relay
The DNS Relayer 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
Internet

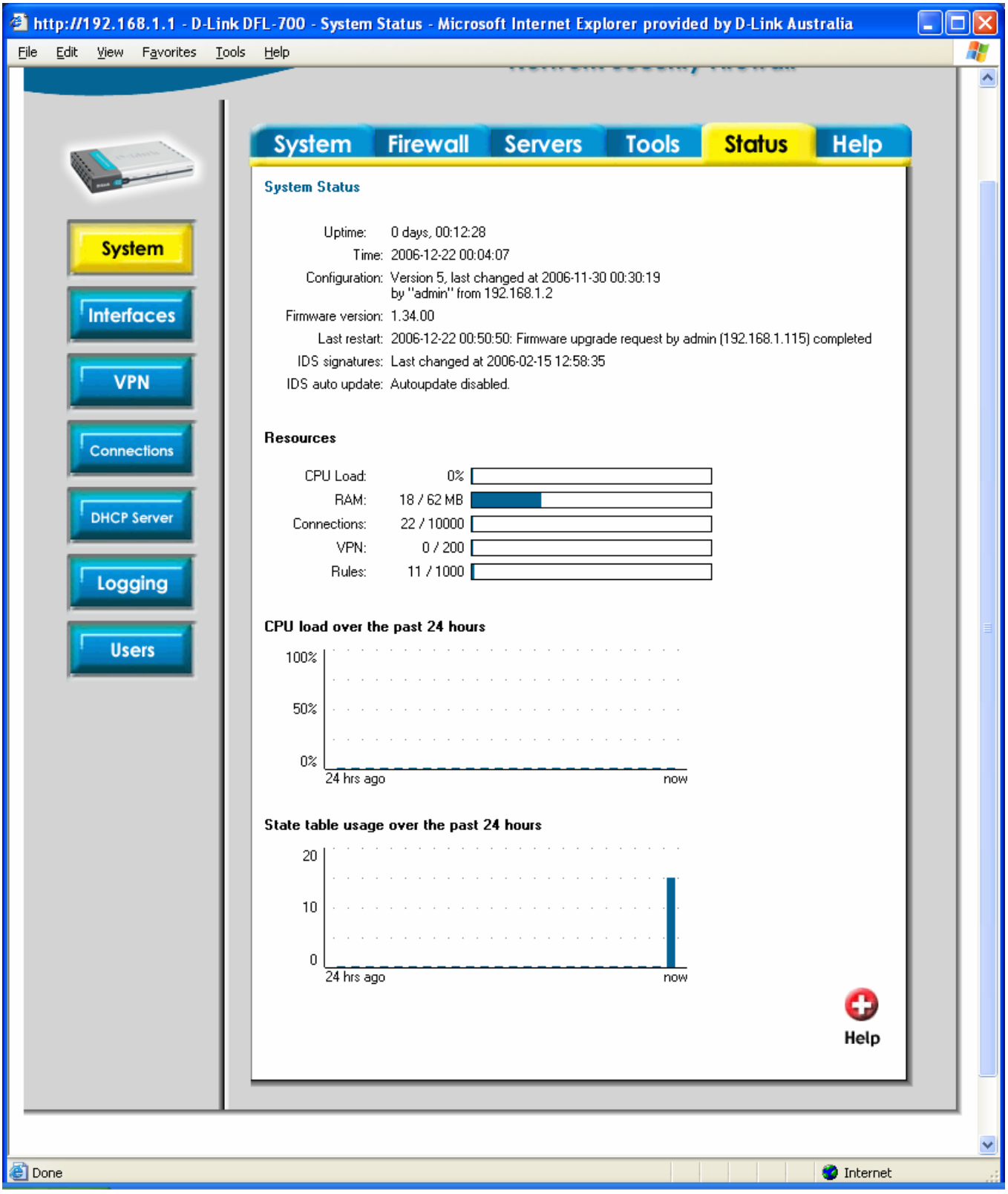

http://192.168.1.1 - D-Link DFL-700 - Ping - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System Firewall Servers Tools Status Help
Ping
DynDNS
Backup
Reset
Upgrade
Ping
IP Address:
Number of packets: 4
Packet size: 32
Apply Cancel Help
Internet

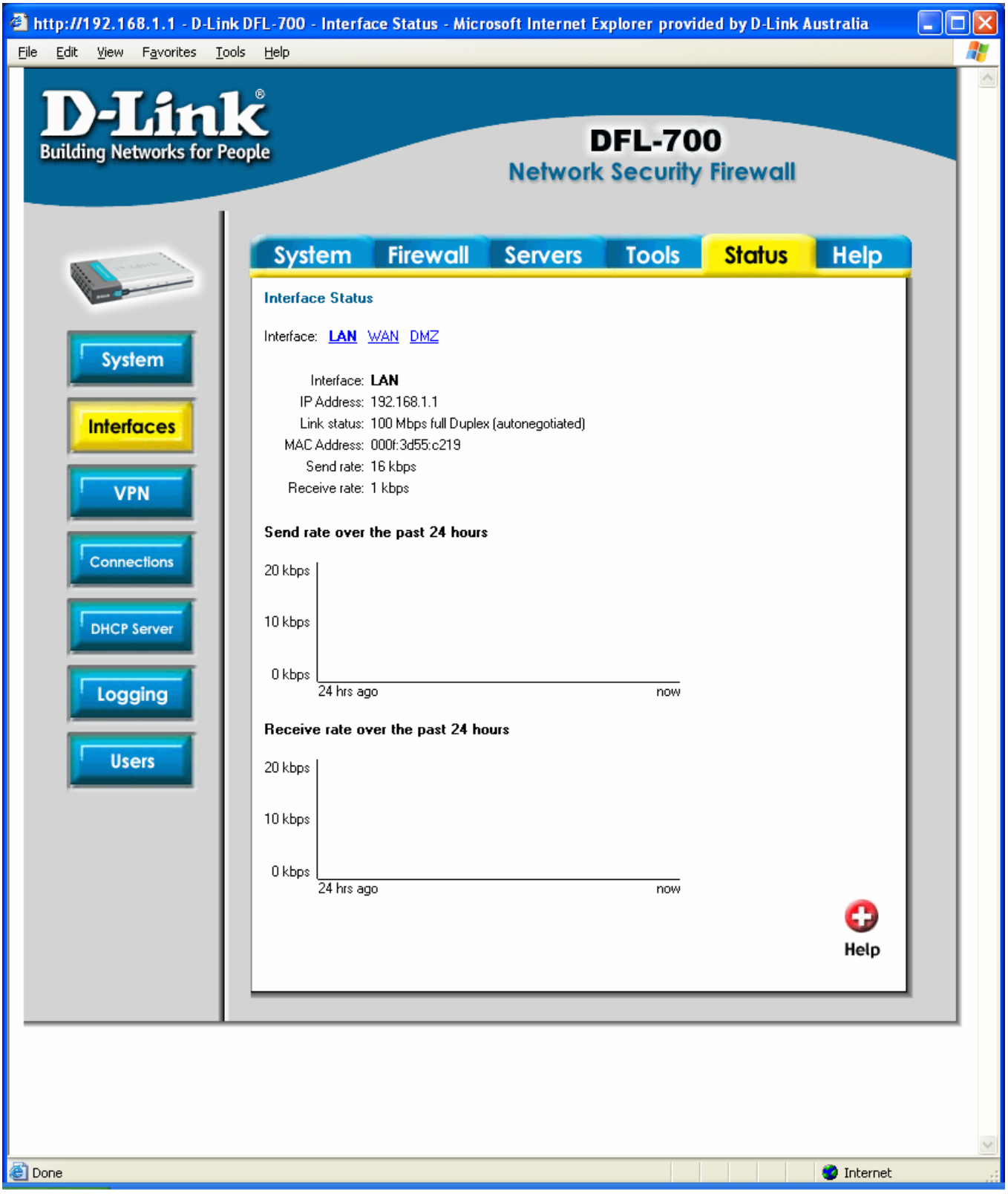

http://192.168.1.1 - D-Link DFL-700 - Dynamic DNS Registration via HTTP - Microsoft Internet Explorer provided by ...
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Ping
DynDNS
Backup
Reset
Upgrade
System Firewall Servers Tools Status Help
Dynamic 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: 14400 minutes
Example: http://user:pass@svc.example.com/path?arg1=val1&arg2=val2
Apply
Cancel
Help
Internet

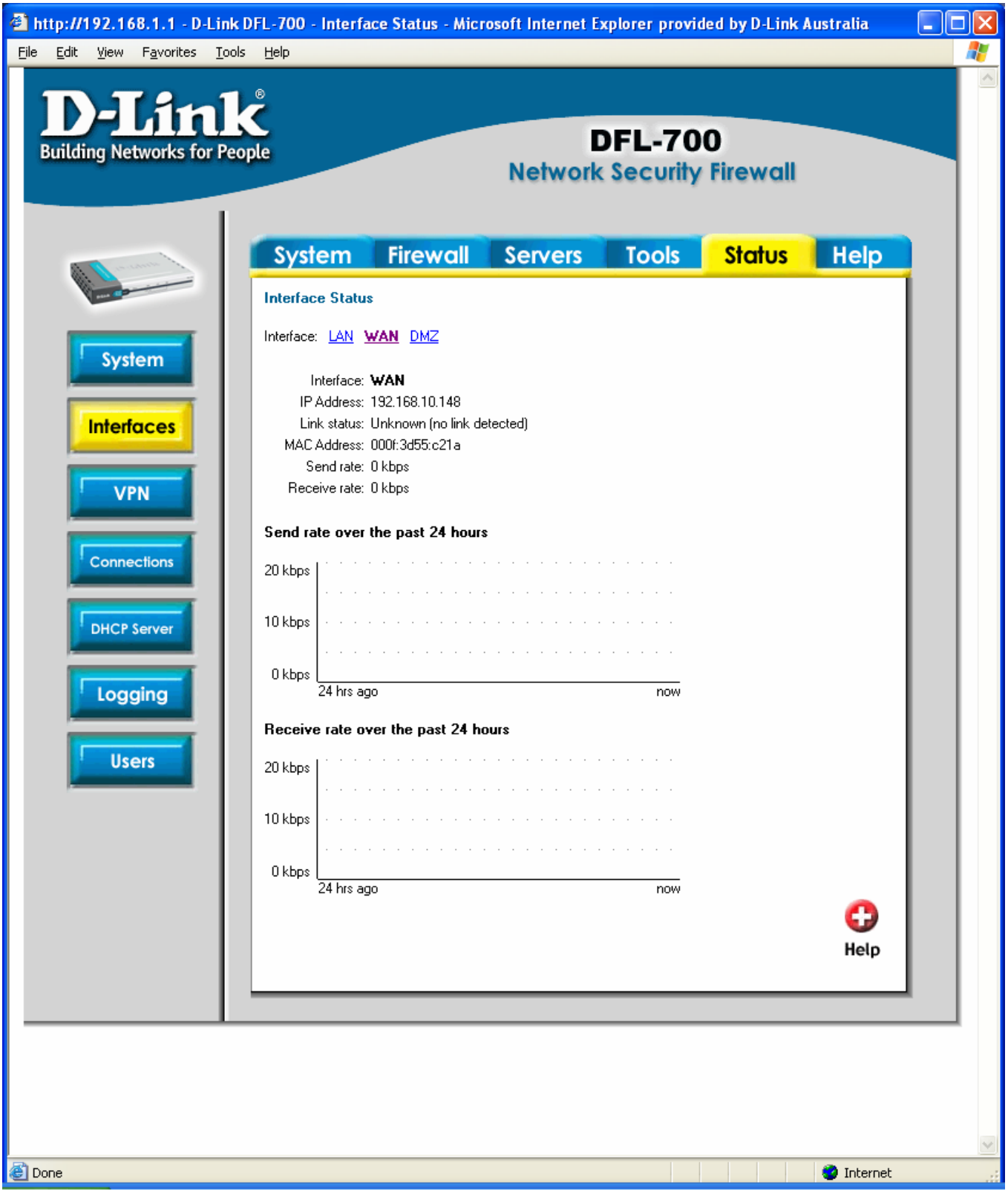

http://192.168.1.1 - D-Link DFL-700 - Backup / Restore - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Ping
DynDNS
Backup
Reset
Upgrade
System Firewall Servers Tools Status Help
Backup / 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
Done
Internet

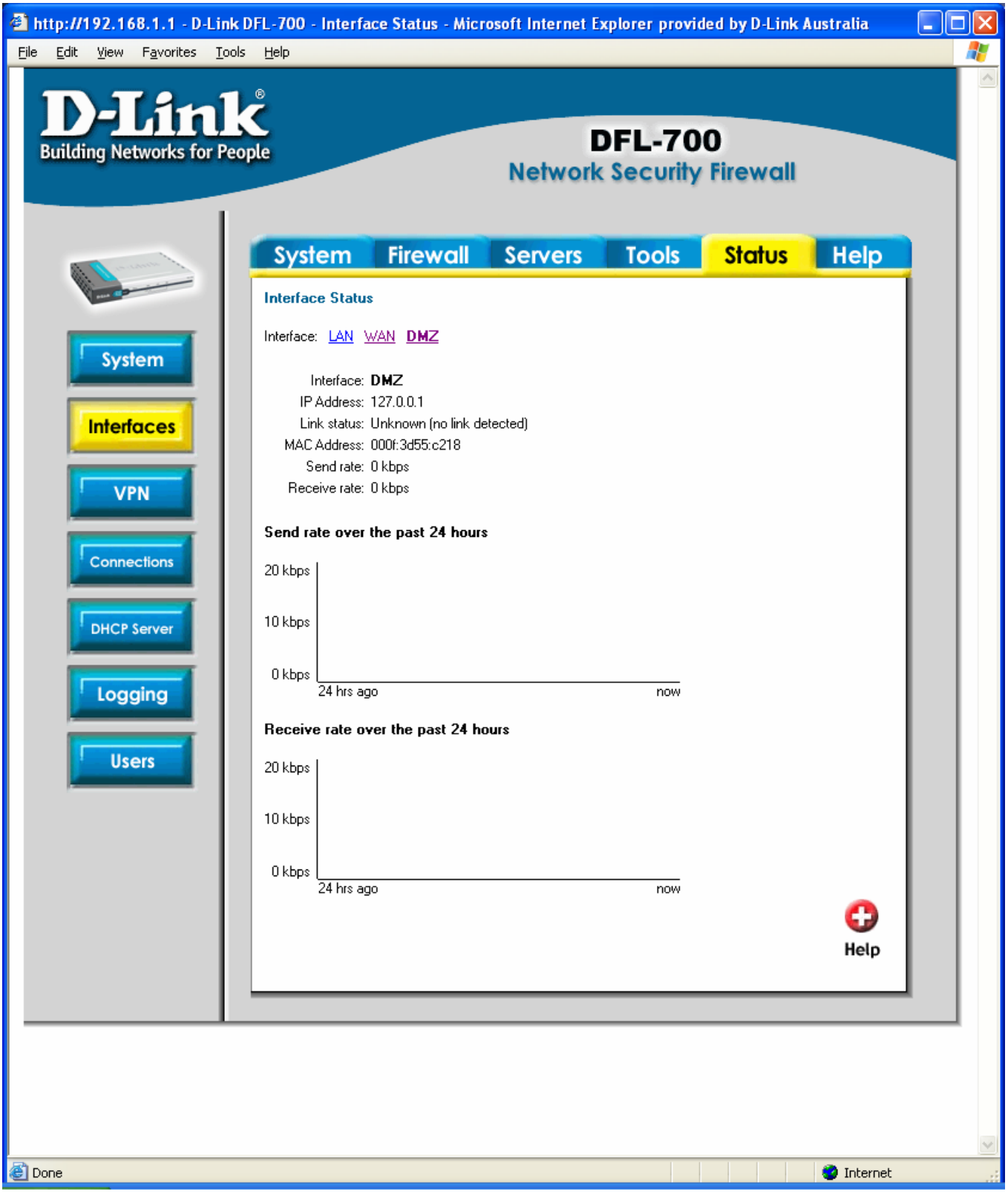

http://192.168.1.1 - D-Link DFL-700 - Restart / Reset - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Ping
DynDNS
Backup
Reset
Upgrade
System Firewall Servers Tools Status Help
Restart / 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 the configuration will be restored to the factory default.
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
Internet

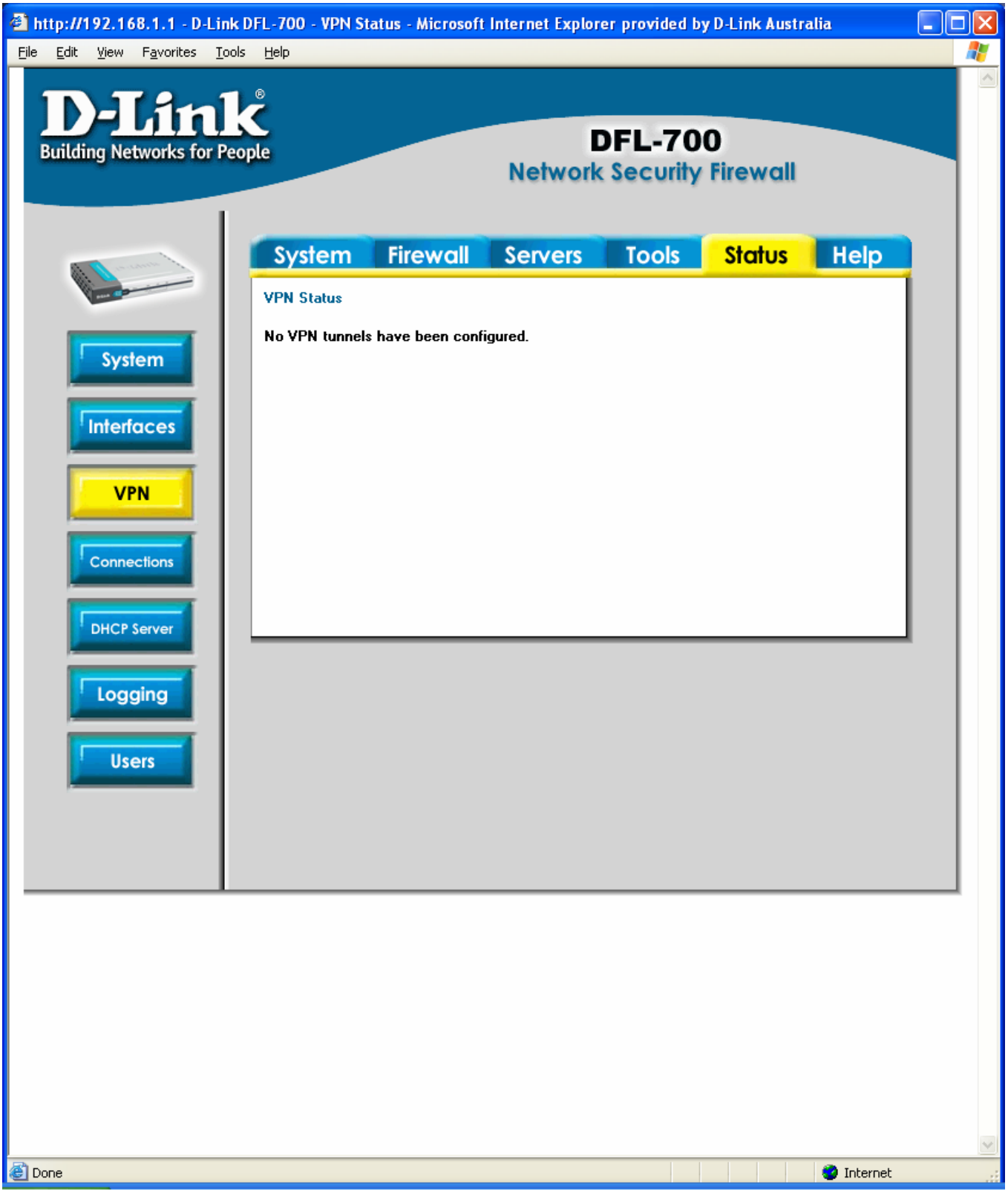

http://192.168.1.1 - D-Link DFL-700 - Upgrade - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
Ping
DynDNS
Backup
Reset
Upgrade
System Firewall Servers Tools Status Help
Upgrade
Upgrade 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.
Note! This will take a few moments.
Warning! Never remove power or reset the unit during the firmware upgrade process.
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
Internet


http://192.168.1.1 - D-Link DFL-700 - System Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
System Status
Uptime: 0 days, 00:12:28
Time: 2006-12-22 00:04:07
Configuration: Version 5, last changed at 2006-11-30 00:30:19 by "admin" from 192.168.1.2
Firmware version: 1.34.00
Last restart: 2006-12-22 00:50:50: Firmware upgrade request by admin (192.168.1.115) completed
IDS signatures: Last changed at 2006-02-15 12:58:35
IDS auto update: Autoupdate disabled.
Resources
CPU Load: 0%
RAM: 18 / 62 MB
Connections: 22 / 10000
VPN: 0 / 200
Rules: 11 / 1000
CPU load over the past 24 hours
100%
50%
0%
24 hrs ago
now
State table usage over the past 24 hours
20
10
0
24 hrs ago
now
Help
Done
Internet

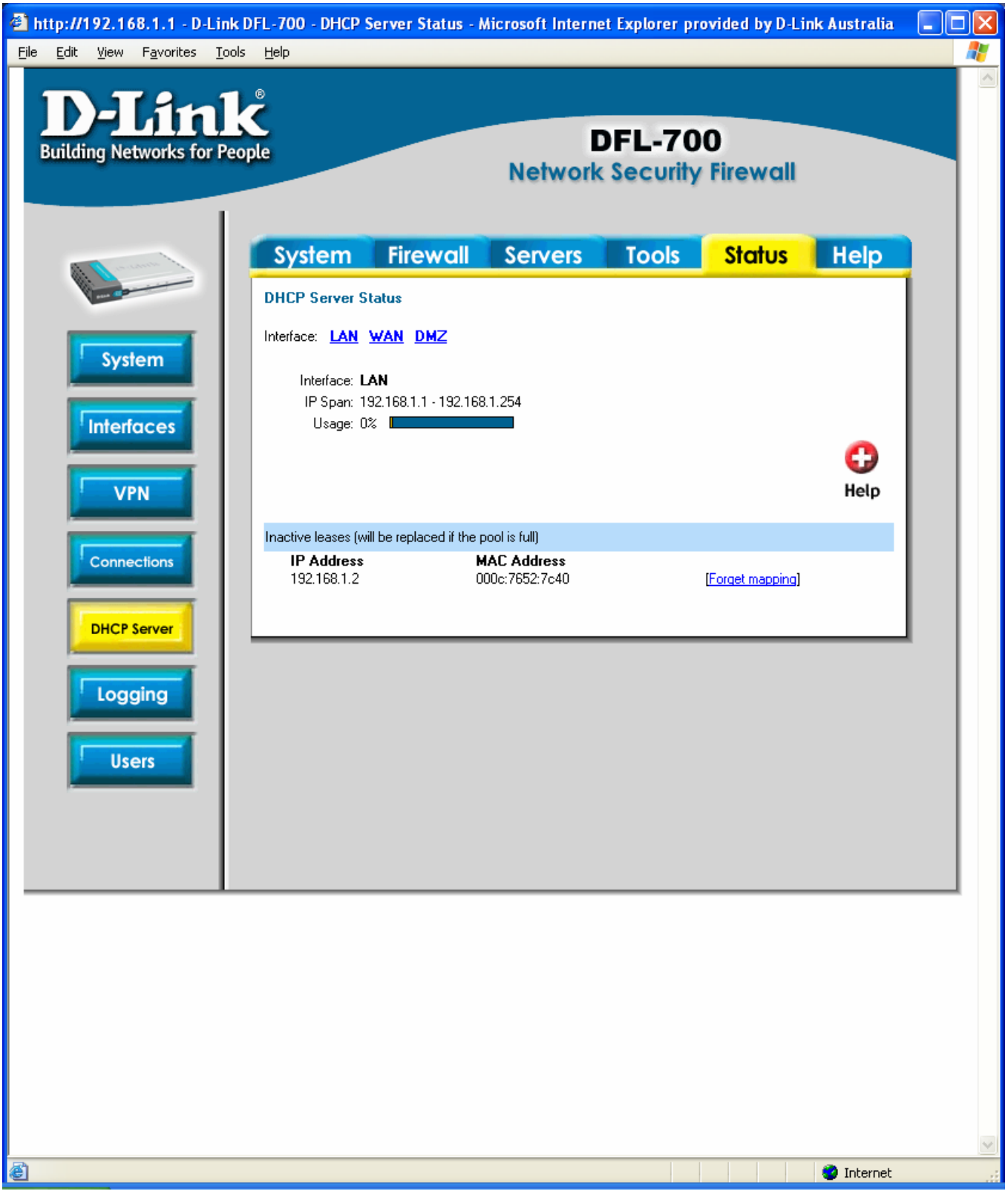

http://192.168.1.1 - D-Link DFL-700 - Interface Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
Interface Status
Interface: LAN WAN DMZ
Interface: LAN
IP Address: 192.168.1.1
Link status: 100 Mbps full Duplex (autonegotiated)
MAC Address: 000f:3d55:c219
Send rate: 16 kbps
Receive rate: 1 kbps
Send rate over the past 24 hours
20 kbps
10 kbps
0 kbps
24 hrs ago
now
Receive rate over the past 24 hours
20 kbps
10 kbps
0 kbps
24 hrs ago
now
Help
Done
Internet

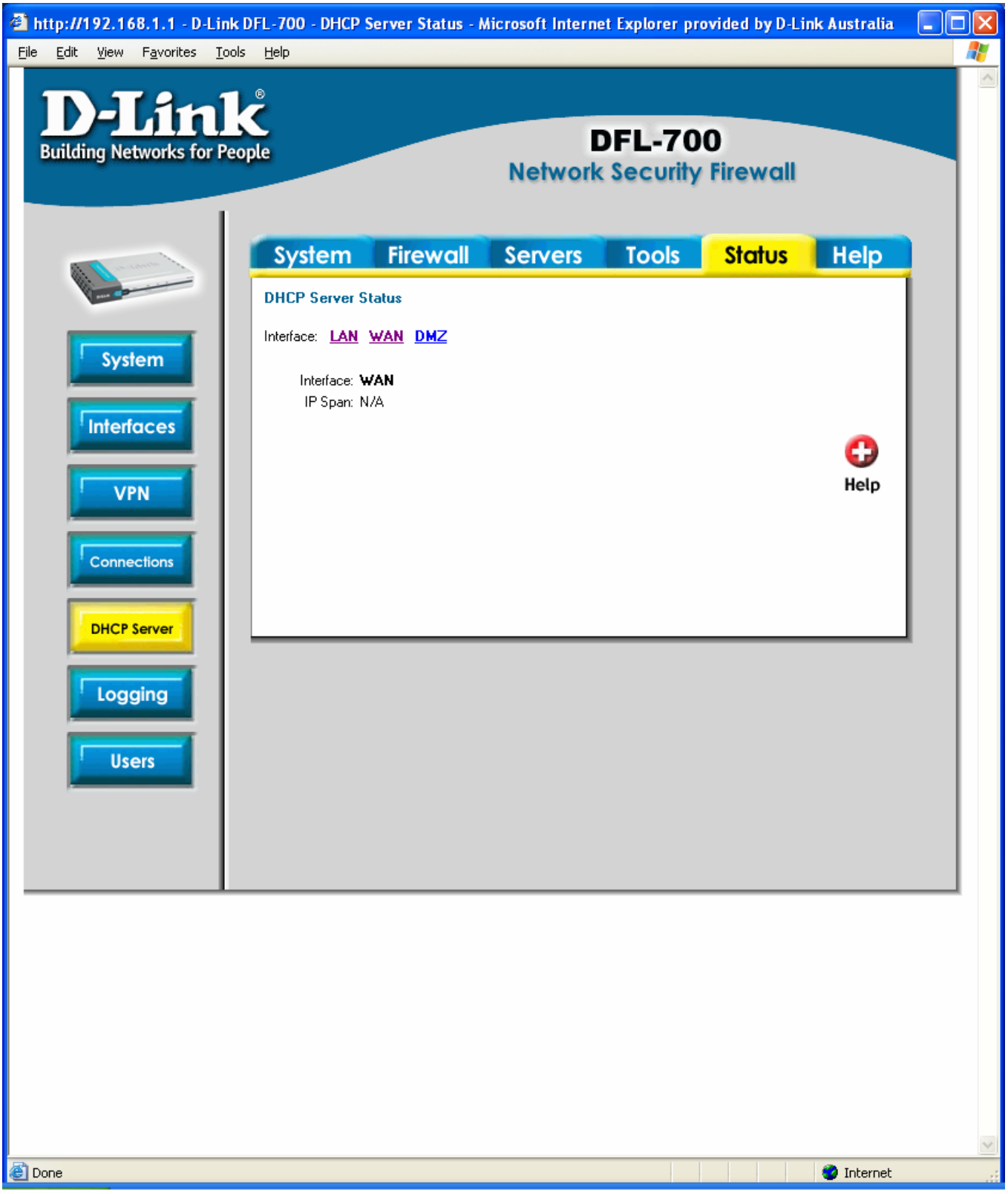

http://192.168.1.1 - D-Link DFL-700 - Interface Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
Interface Status
Interface: LAN WAN DMZ
Interface: WAN
IP Address: 192.168.10.148
Link status: Unknown (no link detected)
MAC Address: 000f:3d55:c21a
Send rate: 0 kbps
Receive rate: 0 kbps
Send rate over the past 24 hours
20 kbps
10 kbps
0 kbps
24 hrs ago
now
Receive rate over the past 24 hours
20 kbps
10 kbps
0 kbps
24 hrs ago
now
Help
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Interface Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
Interface Status
Interface: LAN WAN DMZ
Interface: DMZ
IP Address: 127.0.0.1
Link status: Unknown (no link detected)
MAC Address: 000f:3d55:c218
Send rate: 0 kbps
Receive rate: 0 kbps
Send rate over the past 24 hours
20 kbps
10 kbps
0 kbps
24 hrs ago
now
Receive rate over the past 24 hours
20 kbps
10 kbps
0 kbps
24 hrs ago
now
Help
Done
Internet

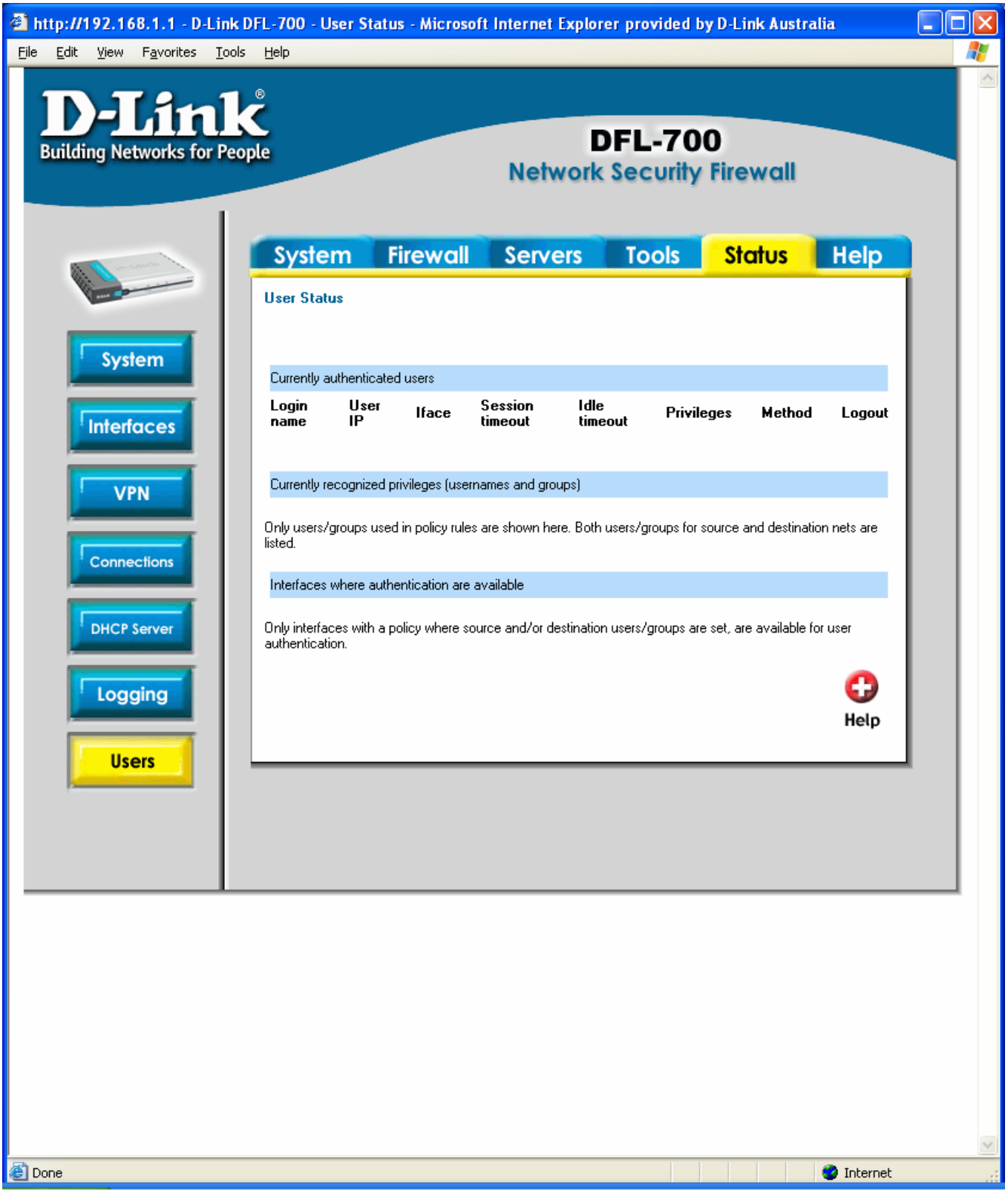

http://192.168.1.1 - D-Link DFL-700 - VPN Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
VPN Status
No VPN tunnels have been configured.
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - State Table Contents - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
State Table Contents
Filter state table display:
Source
Destination
IP Address:
Interface: Any Any
IP Protocol Any
Port:
Apply
Help
State table contents (max 100 entries)
State Proto Source Destination Timeout
PING ICMP LAN:192.168.1.115:768 core:192.168.1.1:768 8
FIN_RCVD TCP LAN:192.168.1.115:4179 core:192.168.1.1:80 28
FIN_RCVD TCP LAN:192.168.1.115:4180 core:192.168.1.1:80 28
FIN_RCVD TCP LAN:192.168.1.115:4183 core:192.168.1.1:80 42
FIN_RCVD TCP LAN:192.168.1.115:4181 core:192.168.1.1:80 36
FIN_RCVD TCP LAN:192.168.1.115:4188 core:192.168.1.1:80 52
FIN_RCVD TCP LAN:192.168.1.115:4191 core:192.168.1.1:80 67
FIN_RCVD TCP LAN:192.168.1.115:4185 core:192.168.1.1:80 46
FIN_RCVD TCP LAN:192.168.1.115:4189 core:192.168.1.1:80 63
FIN_RCVD TCP LAN:192.168.1.115:4178 core:192.168.1.1:80 19
FIN_RCVD TCP LAN:192.168.1.115:4192 core:192.168.1.1:80 71
FIN_RCVD TCP LAN:192.168.1.115:4174 core:192.168.1.1:80 1
FIN_RCVD TCP LAN:192.168.1.115:4173 core:192.168.1.1:80 1
FIN_RCVD TCP LAN:192.168.1.115:4190 core:192.168.1.1:80 63
FIN_RCVD TCP LAN:192.168.1.115:4175 core:192.168.1.1:80 2
FIN_RCVD TCP LAN:192.168.1.115:4182 core:192.168.1.1:80 36
FIN_RCVD TCP LAN:192.168.1.115:4184 core:192.168.1.1:80 42
FIN_RCVD TCP LAN:192.168.1.115:4193 core:192.168.1.1:80 76
TCP_OPEN TCP LAN:192.168.1.115:4194 core:192.168.1.1:80 262144
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - DHCP Server Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
DHCP Server Status
Interface: LAN WAN DMZ
Interface: LAN
IP Span: 192.168.1.1 - 192.168.1.254
Usage: 0%
Help
Inactive leases (will be replaced if the pool is full)
IP Address
MAC Address
192.168.1.2
000c:7652:7c40
[Forget mapping]
Internet


http://192.168.1.1 - D-Link DFL-700 - DHCP Server Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
DHCP Server Status
Interface: LAN WAN DMZ
Interface: WAN
IP Span: N/A
Help
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - Log Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
Log Status
Help
Clear log
Internal Logging (entries 1--100)
Next 100 >>
[2006-12-22 00:04:56] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4205 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:55] <5>EFW: CONN: prio=2 rule=Rule_5 conn=close connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4178 conndestif=core conndestip=192.168.1.1 conndestport=80 origsent=841 termsent=10786
[2006-12-22 00:04:55] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4204 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:49] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4201 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:48] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4200 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:47] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4199 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:46] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4198 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:45] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4197 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:39] <5>EFW: CONN: prio=2 rule=Rule_5 conn=open connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4196 conndestif=core conndestip=192.168.1.1 conndestport=80
[2006-12-22 00:04:38] <5>EFW: CONN: prio=2 rule=Rule_5 conn=close connipproto=TCP connrecvif=LAN connsrcip=192.168.1.115 connsrcport=4175 conndestif=core conndestip=192.168.1.1 conndestport=80 origsent=619 termsent=3671
Done
Internet


http://192.168.1.1 - D-Link DFL-700 - User Status - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
D-Link
Building Networks for People
DFL-700
Network Security Firewall
System
Interfaces
VPN
Connections
DHCP Server
Logging
Users
System Firewall Servers Tools Status Help
User Status
Currently authenticated users
Login name
User IP
Iface
Session timeout
Idle timeout
Privileges
Method
Logout
Currently recognized privileges (usernames and groups)
Only users/groups used in policy rules are shown here. Both users/groups for source and destination nets are listed.
Interfaces where authentication are available
Only interfaces with a policy where source and/or destination users/groups are set, are available for user authentication.
Help
Done
Internet

http://192.168.1.1 - D-Link DFL-700 - Help - Microsoft Internet Explorer provided by D-Link Australia

File Edit View Favorites Tools Help

D-Link
Building Networks for People

DFL-700
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

Help

System
- Administration
- Interfaces
- Routing
- 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
- VPN
- Connections
- DHCP Servers

Done

Internet