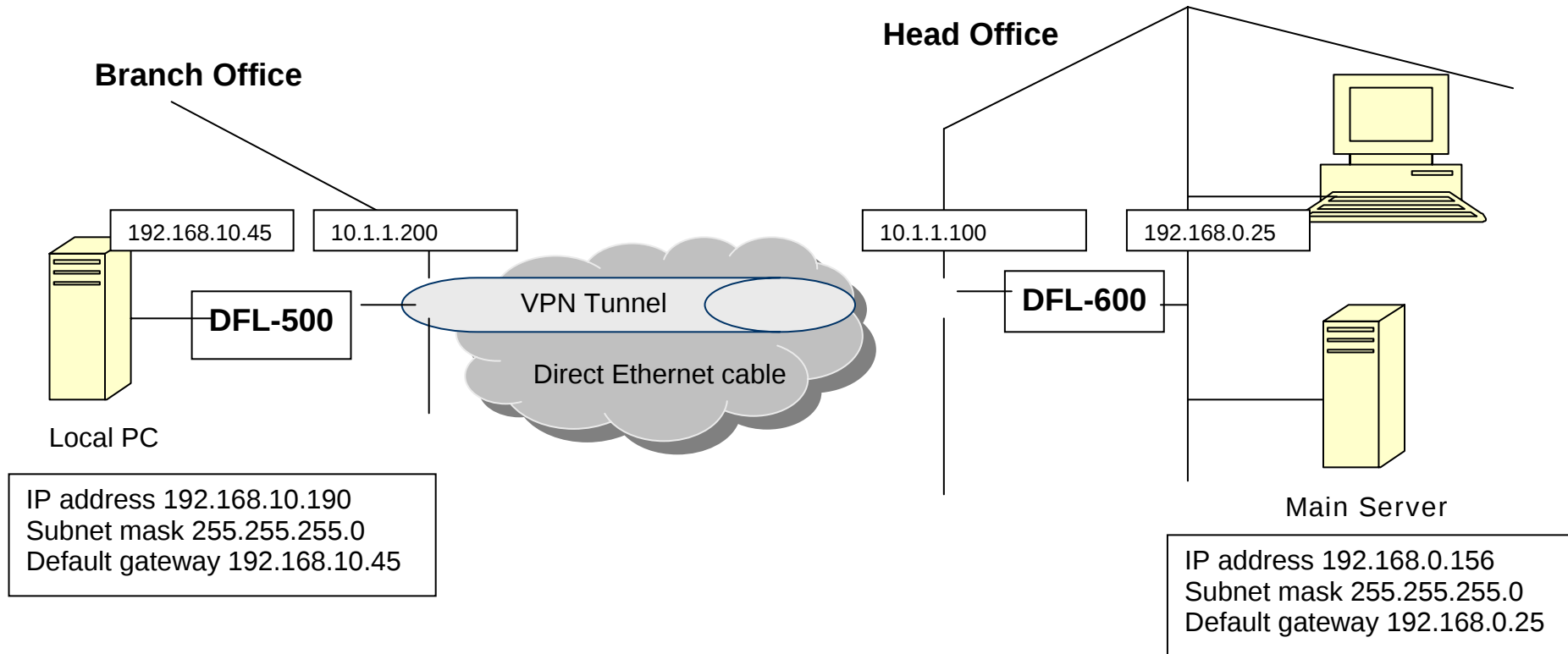




Configuring IPSec VPN between DFL-500 and DFL-600 in 15 simple steps

	DFL-500 configuration	DFL-600 configuration
Firmware version	2.36 build 77	1.05.b091
Lan IP	192.168.10.45 255.0.0.0	192.168.0.25 255.0.0.0
Wan IP	10.1.1.200	10.1.1.100
Default gateway	10.1.1.100	10.1.1.200
Pre-shared key	techsup	techsup
Ipssec local id	10.1.1.200	N/A
Ipssec remote id (peer id)	10.1.1.100	N/A



DFL-500 configuration

1. Configuring internal IP addresses on the firewall (192.168.10.45 255.255.255.0)

D-Link Firewall - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media Print Mail

Address <https://192.168.10.45/theme1/index?login=1> Go Links >>

D-Link® Firewall Appliance **DFL-500** Logout Wizard Help

System
Status
Network
Config
Firewall
User
VPN
Web Filter
Log&Report

Interface DNS Routing Table Routing Gateway

Edit Interface(00:05:5D:EF:62:00)

Name

IP

Netmask

Access ☒ HTTPS ☒ PING
☐ SSH ☐ SNMP

OK Cancel

2. Configuring external IP address on the firewall (10.1.1.200, 255.0.0.0)

D-Link®

Firewall Appliance

DFL-500



Logout



Wizard



Help

System

Status

Network

Config

Firewall

User

VPN

Web Filter

Log&Report

Interface

DNS

Routing Table

Routing Gateway

Edit Interface(00:05:5D:EF:62:01)

Name

Addressing mode ☒ Manual ☐ DHCP ☐ PPPoE

IP

Netmask

Access ☒ HTTPS ☒ PING
☐ SSH ☐ SNMP

MTU (bytes)
☐ Fragment outgoing packets greater than MTU.

3. Assigning DNS IP addresses (10.1.1.150, 139.134.5.51)



Firewall Appliance

DFL-500



Logout



Wizard



Help

System

Status

Network

Config

Firewall

User

VPN

Web Filter

Log&Report

Interface

DNS

Routing Table

Routing Gateway

Primary DNS Server:

10.1.1.150

Second DNS Server:

139.134.5.51

Apply

4. Assigning a Routing table (192.168.10.0, 255.255.255.0, 192.168.0.0, 255.255.255.0, 10.1.1.100)

D-Link®

Firewall Appliance

DFL-500



Logout



Wizard



Help

Interface

DNS

Routing Table

Routing Gateway

DHCP

System

Status

Network

Config

Firewall

User

VPN

Web Filter

Log&Report

Edit Policy Router

Source IP 192.168.10.0

Netmask 255.255.255.0

Destination IP 192.168.0.0

Netmask 255.255.255.0

Gateway #1 10.1.1.100

Gateway #2

Gateway #3

Gateway #4

OK

Cancel

5. Assigning a default gateway (10.1.1.100)

D-Link®

Firewall Appliance

DFL-500

 Logout

 Wizard

 Help

System

Status

Network

Config

Firewall

User

VPN

Web Filter

Log&Report

InterfaceDNSRouting Table**Routing Gateway**DHCP

Edit Routing Gateway

Gateway IP10.1.1.100

☐ Dead gateway detection

OKCancel

6. Creating an internal network for the VPN (192.168.10.0, 255.255.255.0)

D-Link®

Firewall Appliance

DFL-500

Logout

Wizard

Help

System

Firewall

Policy

Address

Service

Schedule

Virtual IP

IP Pool

IP/Mac Binding

User

VPN

Web Filter

Log&Report

Internal

External

Group

Name	IP/Netmask	Modify
Internal_All	0.0.0.0/0.0.0.0	
DFL-500	192.168.10.0/255.255.255.0	

New

6. Creating an external network for the VPN (192.168.0.0, 255.255.255.0)

D-Link®

Firewall Appliance

DFL-500



Logout



Wizard



Help

System

Firewall

Policy

Address

Service

Schedule

Virtual IP

IP Pool

IP/Mac Binding

User

VPN

Web Filter

Log&Report

Internal

External

Group

Name	IP/Netmask	Modify
External_All	0.0.0.0/0.0.0.0	
DFL-600	192.168.0.0/255.255.255.0	

New

7. Creating remote gateway for VPN (10.1.1.100, P1 Proposal; 1 – Encryption DES, Authentication MD5, DH Group 2, Keylife 300, pre-shared key techsup, Local ID 10.1.1.200, Peer id 10.1.1.100, Nat-traversal = enabled)

D-Link®

Firewall Appliance

DFL-500



Logout



Wizard



Help

Manual Key

AutoIKE Key

Remote Gateway

Concentrator

Dialup Monitor

System

Firewall

User

VPN

IPSEC

PPTP

L2TP

Web Filter

Log&Report

Edit VPN Gateway

Gateway Name

gw0

Remote
Gateway

Static IP Address

IP Address

10.1.1.100

Mode

☐ Aggressive

☒ Main (ID Protection)

P1 Proposal

1 - Encryption: DES

Authentication: MD5

2 - Encryption: 3DES

Authentication: SHA1



DH Group

1 ☐ 2 ☒ 5 ☐

Keylife:

300 (Seconds)

Authentication:
(Pre-shared Key)

techsup

Local ID

10.1.1.200 (Optional)

Peer ID

10.1.1.100 (Optional)

Nat-traversal

☒ Enable

Keepalive
Frequency

5 (Seconds)

OK

Cancel

8. Creating AutoIKE key 10.1.1.100, P1 Proposal; 1 – Encryption DES, Authentication SHA1.

“Enable” replay detection and perfect forward.

DH Group 1, Keylife 600,

D-Link®

Firewall Appliance

DFL-500

Logout

Wizard

Help

Manual Key

AutoIKE Key

Remote Gateway

Concentrator

Dialup Monitor

System

Status

Network

Config

Firewall

User

VPN

IPSEC

PPTP

L2TP

Web Filter

Log&Report

Edit VPN Tunnel

Tunnel Name

test

Remote Gateway

gw0

P2 Proposal

1-Encryption:

DES

Authentication:

SHA1

2-Encryption:

3DES

Authentication:

SHA1

☒ Enable replay detection

☒ Enable perfect forward secrecy(PFS).

DH Group

1

2

5

Keylife:

Seconds

600

(Seconds)

4608000

(KBytes)

Autokey Keep Alive

☒ Enable

Concentrator

None

OK

Cancel

9. Creating int-to-ext VPN policy

D-Link®

Firewall Appliance

DFL-500

Logout

Wizard

Help

System

Firewall

Policy

Address

Service

Schedule

Virtual IP

IP Pool

IP/Mac Binding

User

VPN

Web Filter

Log&Report

Int->Ext

Ext->Int

Edit Policy

Source DFL-500

Destination DFL-600

Schedule Always

Service ANY

Action ENCRYPT

VPN Tunnel test

☒ Allow inbound

☐ Inbound NAT

☒ Allow outbound

☐ Outbound NAT

☐ Traffic Shaping

Guaranteed Bandwidth 0 (Kbytes/sec)

Maximum Bandwidth 0 (Kbytes/sec)

Traffic Priority High

☐ Log Traffic

☐ Web filter [show settings](#)

OK

Cancel

10. In the Firewall > Policy page then Int -> Ext
Click on the “move to” button next to the DFL-500 to DFL-600 as below

#	Source	Dest	Schedule	Service	Action	Enable	Config
1	DFL-500	DFL-600	Always	ANY	ENCRYPT	☒	
2	Internal_All	External_All	Always	ANY	ACCEPT	☒	

New

Then in current order place in “1” then click OK.

Move Outgoing Policy	
Current Order	1
Move to	
OK	Cancel

The DFL-500 should move to # 1.

11. Creating ext-to-int vpn policy

D-Link®

Firewall Appliance

DFL-500



Logout



Wizard



Help

System

Firewall

Policy

Address

Service

Schedule

Virtual IP

IP Pool

IP/Mac Binding

User

VPN

Web Filter

Log&Report

Int->Ext

Ext->Int

Edit Policy

Source DFL-600

Destination DFL-500

Schedule Always

Service ANY

Action ENCRYPT

VPN Tunnel test

☒ Allow inbound ☐ Inbound NAT

☒ Allow outbound ☐ Outbound NAT

☐ Traffic Shaping

Guaranteed Bandwidth 0 (Kbytes/sec)

Maximum Bandwidth 0 (Kbytes/sec)

Traffic Priority High

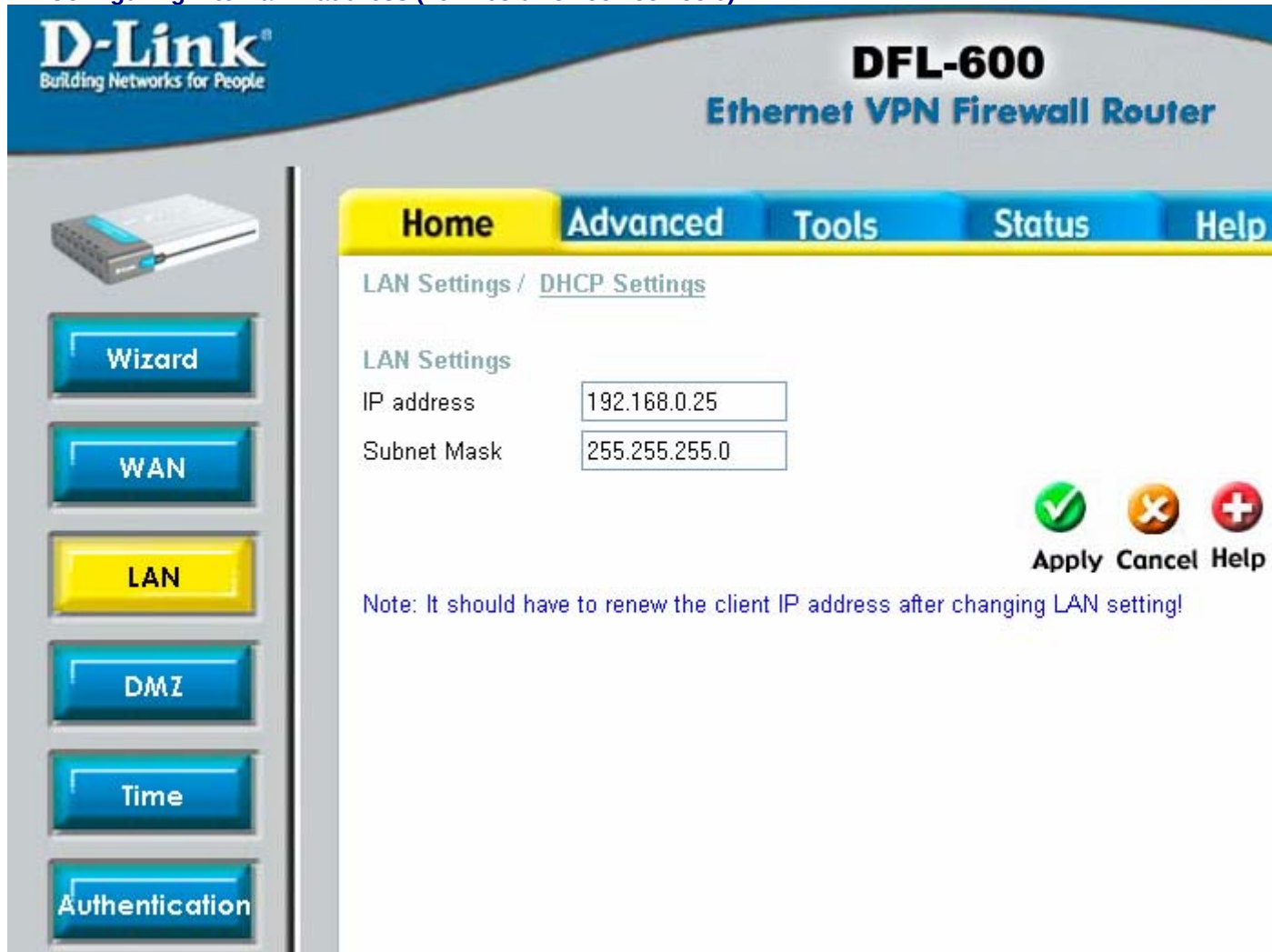
☐ Log Traffic

OK

Cancel

DFL-600 configuration

12. Configuring internal IP address (192.168.0.25 255.255.255.0)



The image shows the web-based configuration interface for a D-Link DFL-600 Ethernet VPN Firewall Router. The interface has a blue header with the D-Link logo and the product name. A navigation bar at the top includes tabs for Home, Advanced, Tools, Status, and Help. On the left side, there is a vertical menu with buttons for Wizard, WAN, LAN (which is highlighted in yellow), DMZ, Time, and Authentication. The main content area is titled 'LAN Settings / DHCP Settings'. Under 'LAN Settings', there are two input fields: 'IP address' with the value '192.168.0.25' and 'Subnet Mask' with the value '255.255.255.0'. To the right of these fields are three circular icons: a green checkmark, an orange 'X', and a red plus sign. Below these icons are the labels 'Apply', 'Cancel', and 'Help'. At the bottom of the main content area, there is a note: 'Note: It should have to renew the client IP address after changing LAN setting!'.

D-Link®
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

Home Advanced Tools Status Help

LAN Settings / DHCP Settings

LAN Settings

IP address 192.168.0.25

Subnet Mask 255.255.255.0

✓ ✗ +
Apply Cancel Help

Note: It should have to renew the client IP address after changing LAN setting!

13. Configuring external IP address, default gateway and DNS (10.1.1.100, 255.0.0.0, 10.1.1.200, 10.1.1.150)

**DFL-600**
Ethernet VPN Firewall Router


Wizard
WAN
LAN
DMZ
Time
Authentication

Home **Advanced** **Tools** **Status** **Help**

WAN Settings

IP settings Mode	Static
IP address	10.1.1.100
Subnet Mask	255.0.0.0
Default Gateway	10.1.1.200
Primary DNS Server	10.1.1.150
Secondary DNS Server	139.134.5.51 (Optional)

  
Apply **Cancel** **Help**

14. Make sure IPSec Status is Enabled.



The screenshot displays the web management interface of a D-Link DFL-600 Ethernet VPN Firewall Router. The interface features a blue header with the D-Link logo and the product name. A left sidebar contains a vertical menu with buttons for NAT, Routing, Policy, VPN-IPSec (highlighted in yellow), VPN-PPTP, VPN-L2TP, and DDNS. The main content area has a top navigation bar with tabs for Home, Advanced (selected), Tools, Status, and Help. Below the tabs, a breadcrumb trail shows the path: IPSec Settings / Tunnel Settings / Tunnel Table / IPSec Status. The main content area contains two settings: "IPSec Passthrough" with an unchecked checkbox and "IPSec Status" with a checked checkbox, both labeled "Enable". At the bottom right, there are three circular icons: a green checkmark, an orange 'X', and a red plus sign, with the labels "Apply", "Cancel", and "Help" respectively.

D-Link®
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

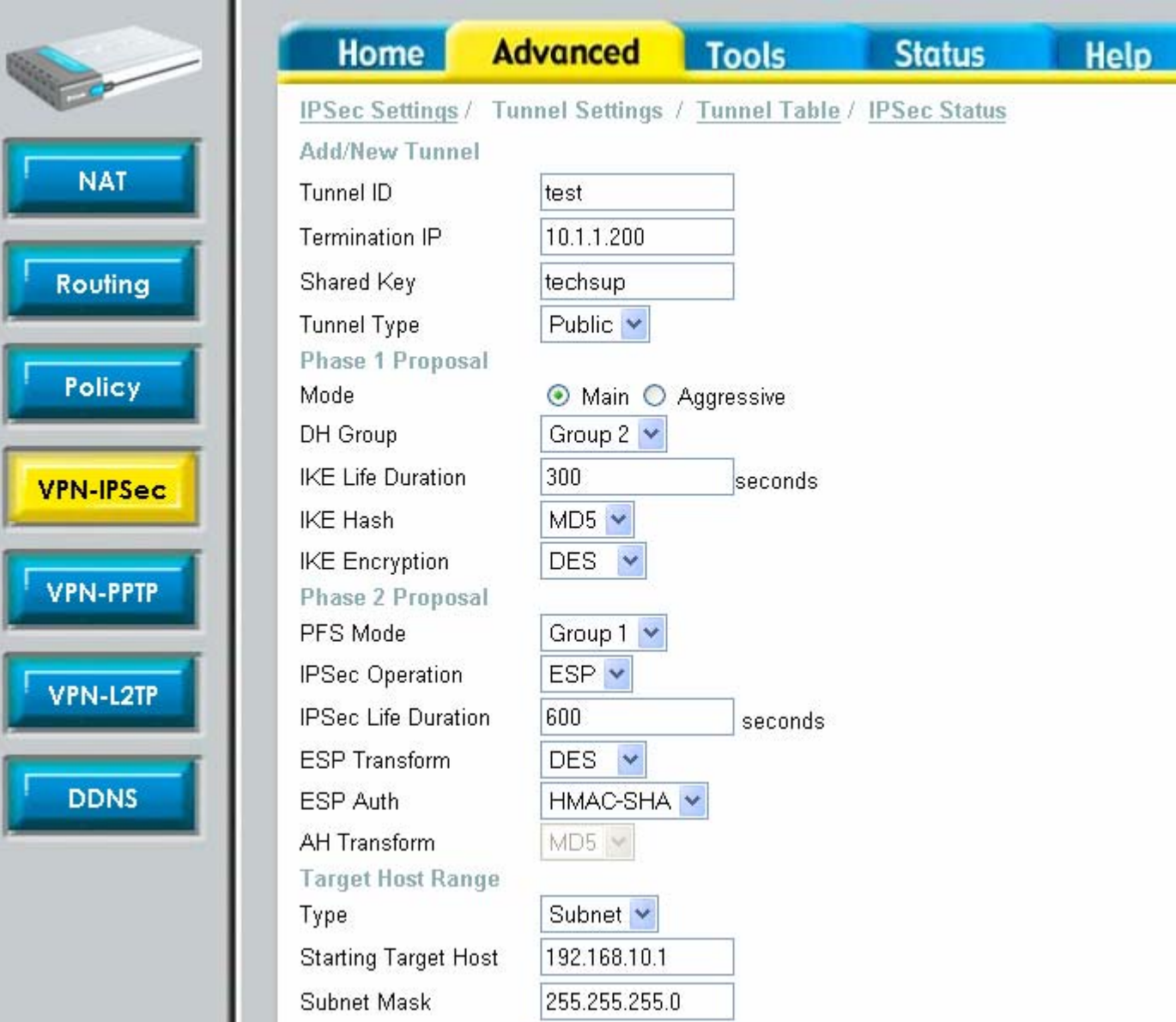
Home Advanced Tools Status Help

IPSec Settings / Tunnel Settings / Tunnel Table / IPSec Status

IPSec Passthrough ☐ Enable
IPSec Status ☒ Enable

Apply Cancel Help

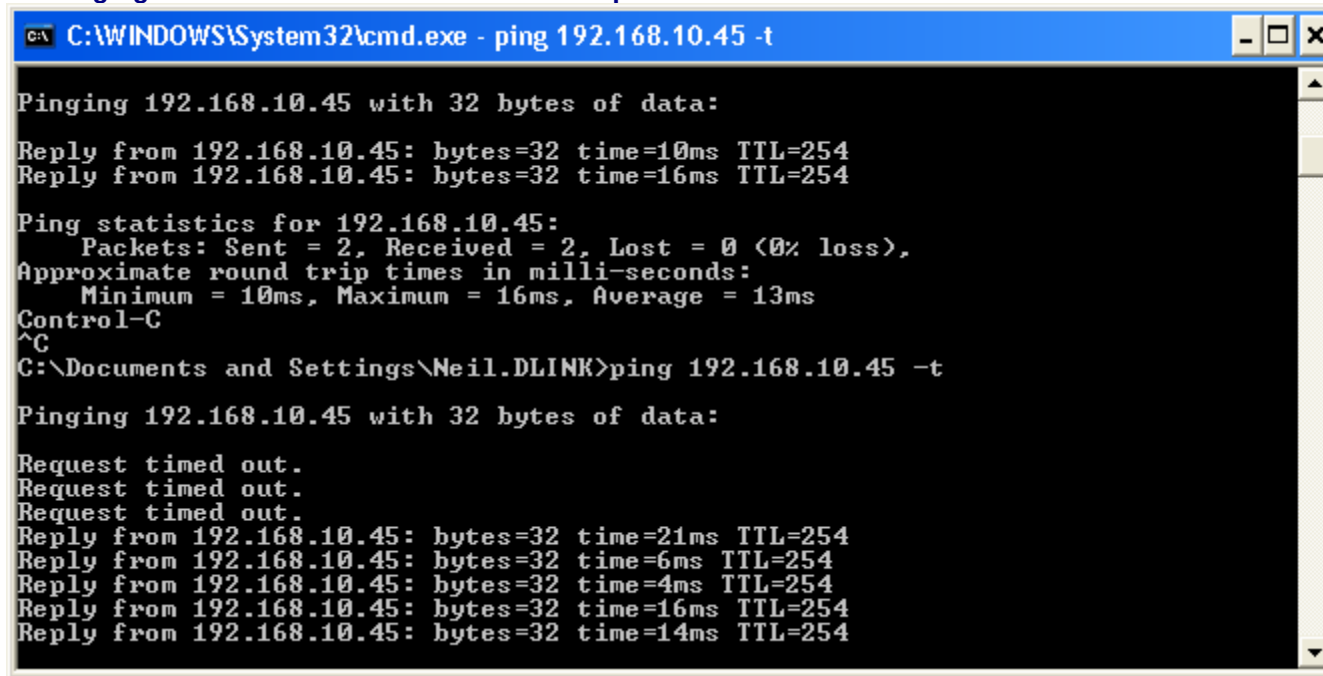
15. Configuring VPN (Termination IP 10.1.1.200, Shared Key techsup. PHASE 1 setup; DH Group 2, IKE Life 300, IKE Hash MD5, IEK Encryption DES Phase 2 setup; PFS mode Group 1, IPSec Operation ESP, IPSec Life 600, ESP Transform DES, ESP Auth HMAC-SHA. Target Host Range setup; Starting target Host 192.168.10.1, Subnet 255.255.255.0



The image shows a web-based configuration interface for a VPN. On the left is a sidebar with navigation buttons: NAT, Routing, Policy, VPN-IPSec (highlighted in yellow), VPN-PPTP, VPN-L2TP, and DDNS. Above these buttons is a small image of a VPN device. The main area has a top navigation bar with tabs: Home, Advanced (selected), Tools, Status, and Help. Below the tabs is a breadcrumb trail: [IPSec Settings](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#). The 'Add/New Tunnel' section contains the following fields:

Tunnel ID	test
Termination IP	10.1.1.200
Shared Key	techsup
Tunnel Type	Public
Phase 1 Proposal	
Mode	☒ Main ☐ Aggressive
DH Group	Group 2
IKE Life Duration	300 seconds
IKE Hash	MD5
IKE Encryption	DES
Phase 2 Proposal	
PFS Mode	Group 1
IPSec Operation	ESP
IPSec Life Duration	600 seconds
ESP Transform	DES
ESP Auth	HMAC-SHA
AH Transform	MD5
Target Host Range	
Type	Subnet
Starting Target Host	192.168.10.1
Subnet Mask	255.255.255.0

15. Pinging a PC behind DFL-500 from the local pc behind DFL-600 .



```
C:\WINDOWS\System32\cmd.exe - ping 192.168.10.45 -t

Pinging 192.168.10.45 with 32 bytes of data:
Reply from 192.168.10.45: bytes=32 time=10ms TTL=254
Reply from 192.168.10.45: bytes=32 time=16ms TTL=254

Ping statistics for 192.168.10.45:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 16ms, Average = 13ms
Control-C
^C
C:\Documents and Settings\Neil.DLINK>ping 192.168.10.45 -t

Pinging 192.168.10.45 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.10.45: bytes=32 time=21ms TTL=254
Reply from 192.168.10.45: bytes=32 time=6ms TTL=254
Reply from 192.168.10.45: bytes=32 time=4ms TTL=254
Reply from 192.168.10.45: bytes=32 time=16ms TTL=254
Reply from 192.168.10.45: bytes=32 time=14ms TTL=254
```

Congratulations!