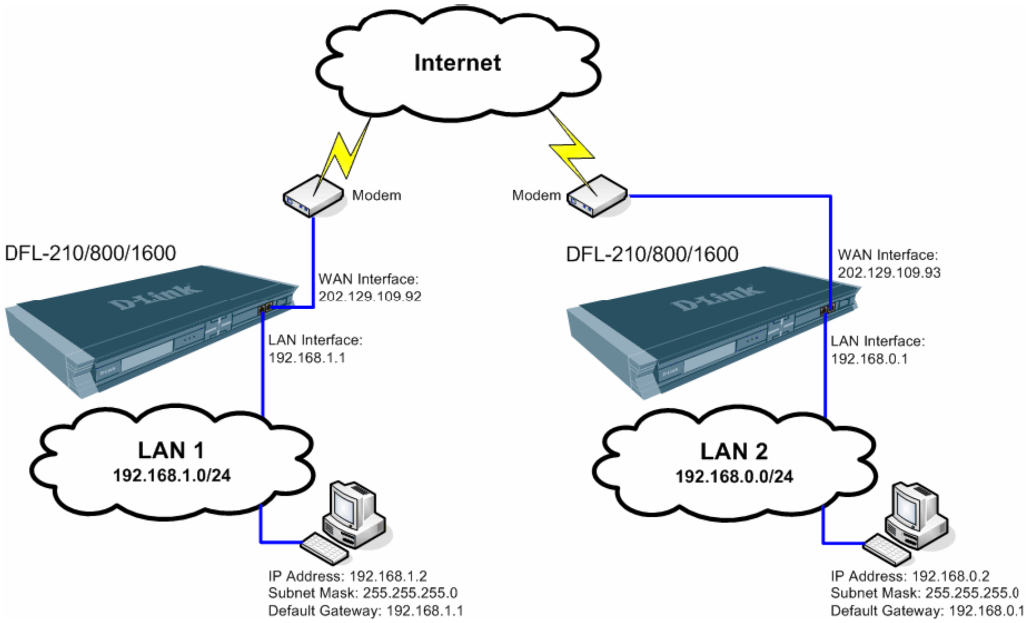
DFL-210/260, DFL-800/860, DFL-1600/2500
How to setup IPSec VPN connection

This setup example uses the following network settings:

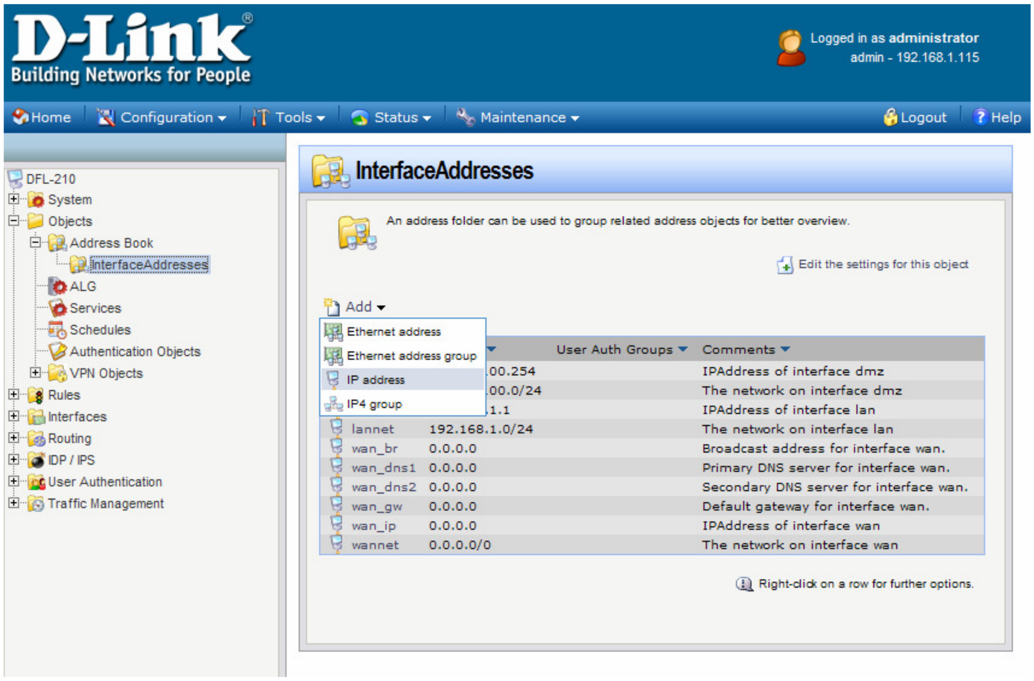


In our example the IPSec VPN tunnel is established between two LANs: 192.168.0.x and 192.168.1.x.
NOTE: It is essential to have private networks (LAN 1 and LAN 2) on different subnets.

Configuration of the Firewall on LAN 1

Step 1. Log into the Firewall by opening Internet Explorer and typing the LAN address of the Firewall. In our example we are using the default 192.168.1.1. Enter Username and Password which you specified during the initial setup of the Firewall.

Step 2. Go to Objects > Address Book > Interface Addresses. Click on Add and select “IP address”.



InterfaceAddresses

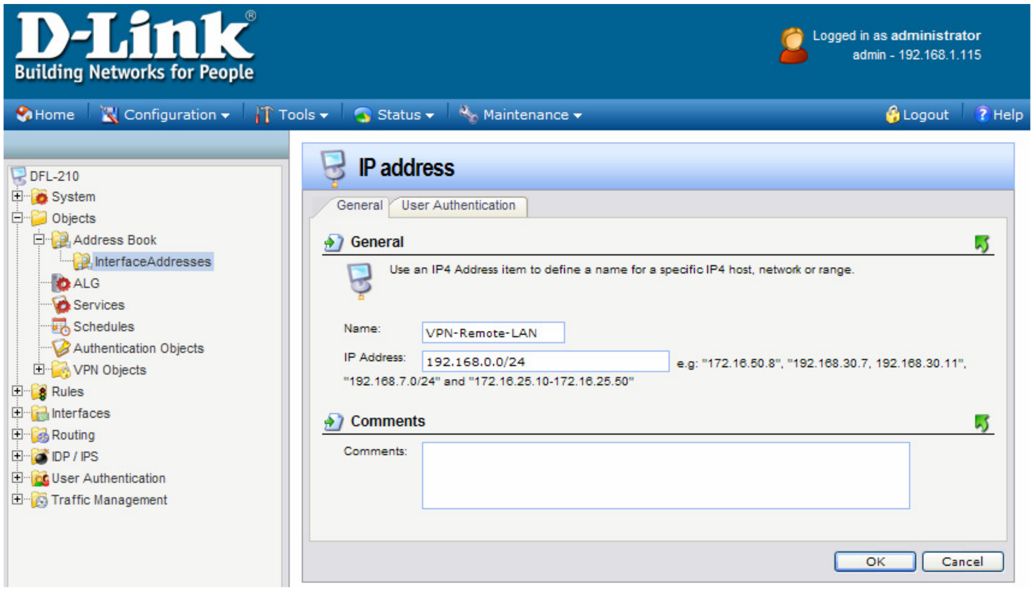
An address folder can be used to group related address objects for better overview.

Edit the settings for this object

		User Auth Groups	Comments
	00.254		IPAddress of interface dmz
	00.0/24		The network on interface dmz
	1.1		IPAddress of interface lan
lannet	192.168.1.0/24		The network on interface lan
wan_br	0.0.0.0		Broadcast address for interface wan.
wan_dns1	0.0.0.0		Primary DNS server for interface wan.
wan_dns2	0.0.0.0		Secondary DNS server for interface wan.
wan_gw	0.0.0.0		Default gateway for interface wan.
wan_ip	0.0.0.0		IPAddress of interface wan
wannet	0.0.0.0/0		The network on interface wan

Right-click on a row for further options.

Specify the settings of the remote network on the other end of the VPN tunnel.
Under Name enter “VPN-Remote-LAN”.
Under IP Address enter the Subnet ID and Mask Bits for the remote network: in our example it is 192.168.0.0/24. Click on the OK button.



IP address

General

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

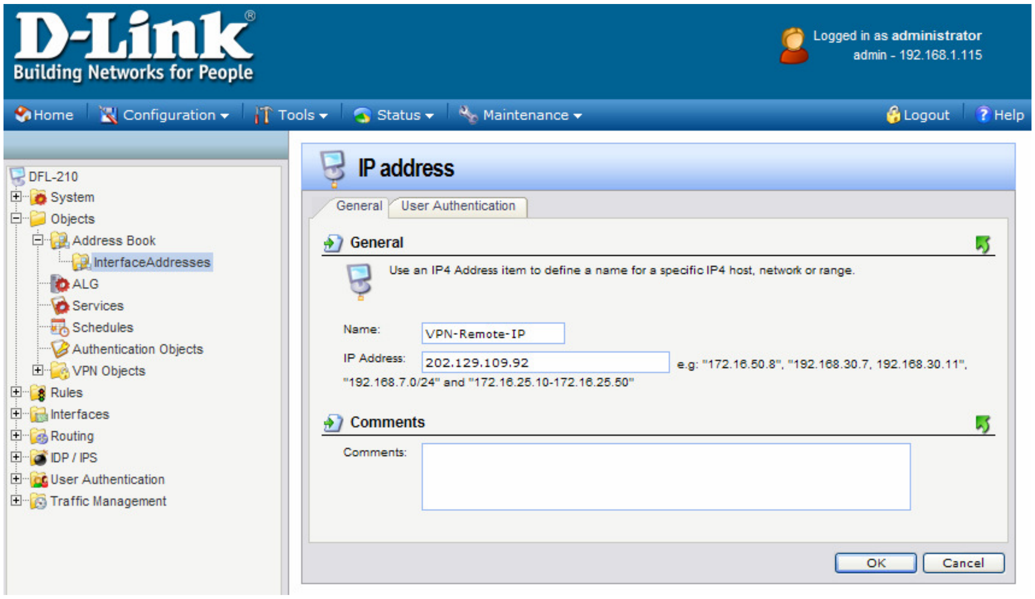
Name: VPN-Remote-LAN

IP Address: 192.168.0.0/24 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments

Comments:

Step 3. Add another “IP Address”. Enter the settings of the VPN endpoint, the public IP address of LAN 2.
Under Name enter “VPN-Remote-IP”.
Under IP address specify the public IP address of the remote network (the IP address assigned by the ISP).



IP address

General

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: VPN-Remote-IP

IP Address: 202.129.109.92 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments

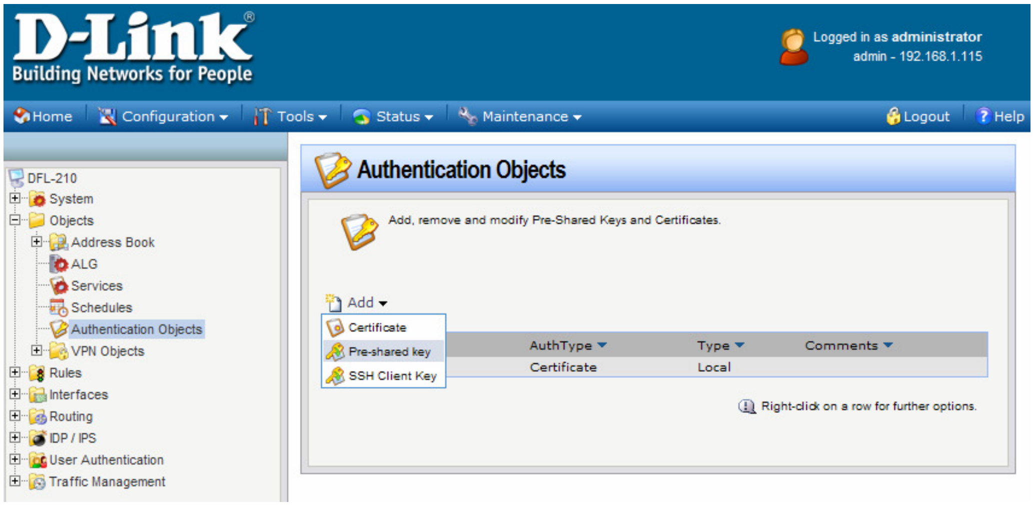
Comments:

***Dynamic IP Address**: If remote network has dynamic public IP address, you can utilize one of the “Dynamic DNS” services available on the Internet. In this case the dynamic IP address of the remote site will be associated with a URL. To specify a URL as an address use this format: **dns:yoursite.dyndns.org**. Type the required URL under Interfaces > IPSec Tunnels > ‘your tunnel settings’ > Remote Endpoint (**Step 5**).*

To configure the VPN firewall to update one of the Dynamic DNS services go to System > Misc. Clients > Add…

*When setting up IPSec VPN Tunnel (**Step 5**) which connects to a site with dynamic IP address or accepts connections from roaming IPSec clients with dynamic IP addresses, set Remote Network as “Any” and Remote Endpoint as “None”.*

Step 4. Go to Object > Authentication Objects > Click on Add and select Pre-Shared Key.



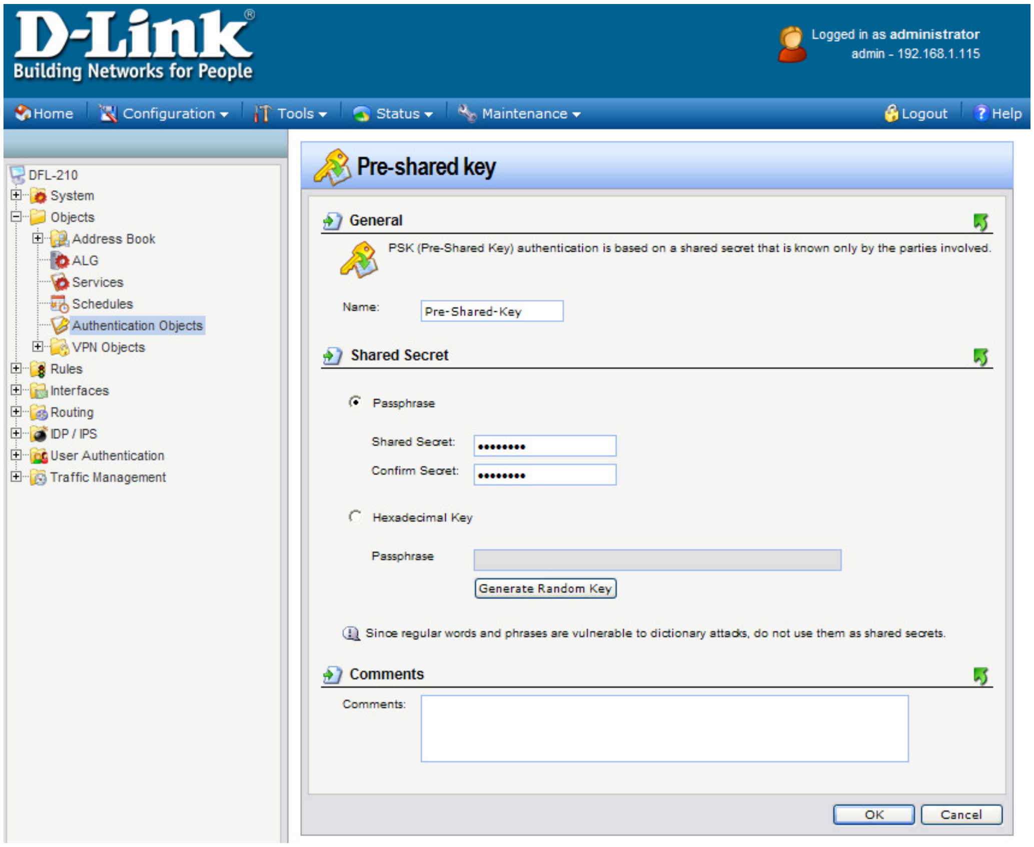
Authentication Objects

Add, remove and modify Pre-Shared Keys and Certificates.

AuthType	Type	Comments
Certificate	Local	

Right-click on a row for further options.

Enter the Pre-Shared Key settings for your VPN tunnel.
Under Name type “Pre-Shared-Key”.
Under Shared Secret select the type of key you want to use and type in the key. In our example we are using ASCII key (passphrase). Note that you will need to use exactly the same key when setting up the firewall on the other end of the tunnel.
Click OK when done.



Pre-shared key

General

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name: Pre-Shared-Key

Shared Secret

● Passphrase

Shared Secret: ••••••••

Confirm Secret: ••••••••

○ Hexadecimal Key

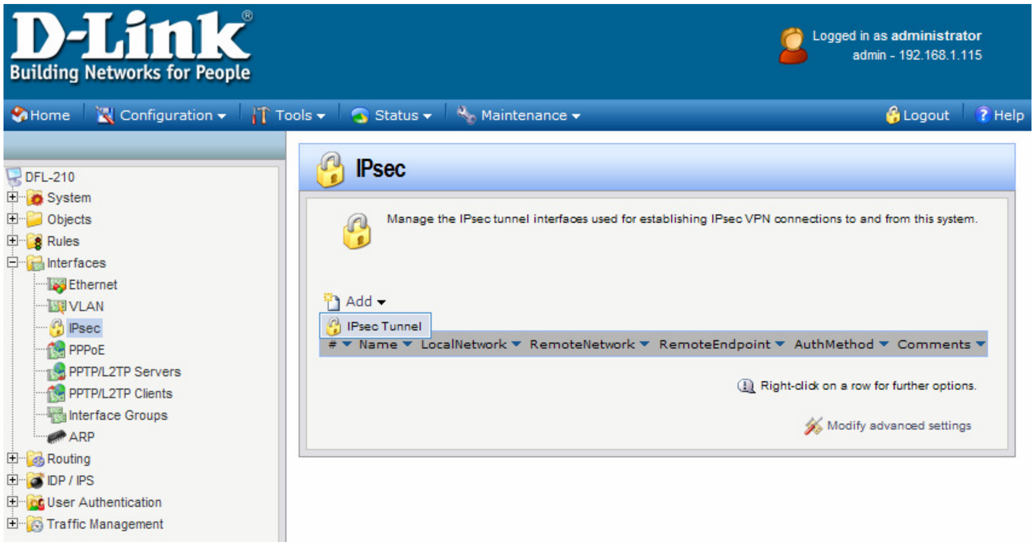
Passphrase:

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Comments

Comments:

Step 5. Go to Interfaces > IPSec. Click on Add and select IPSec Tunnel.

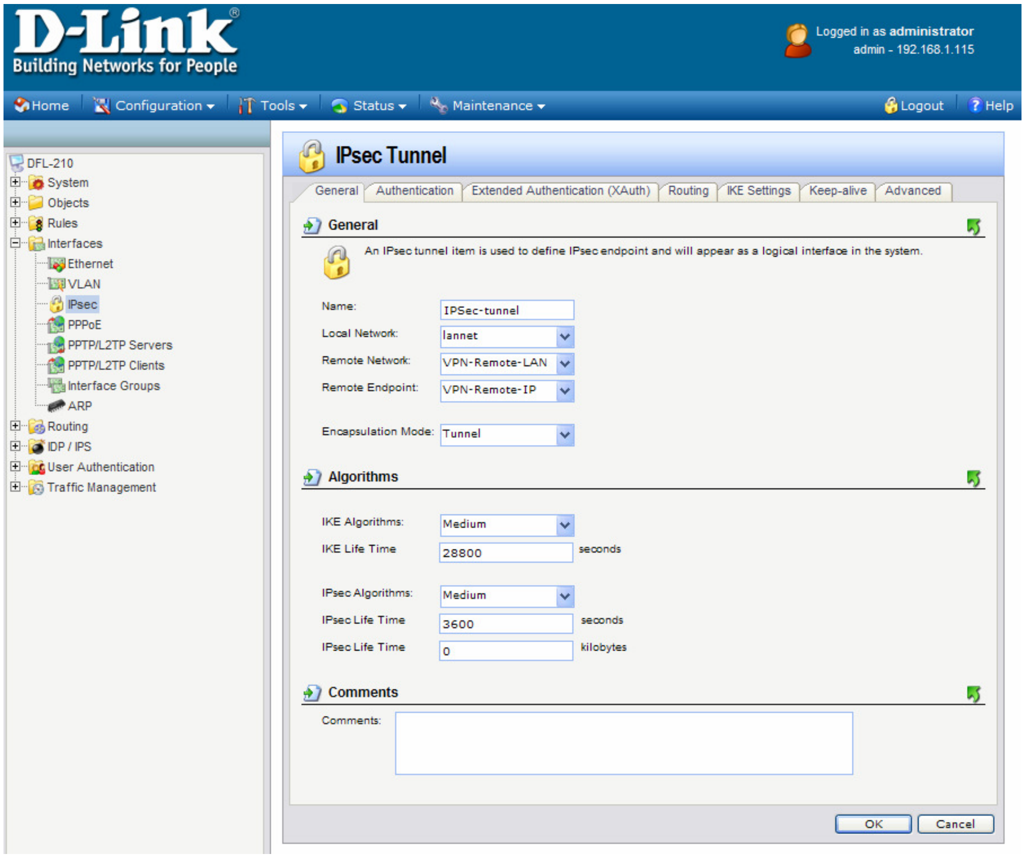


IPsec

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	LocalNetwork	RemoteNetwork	RemoteEndpoint	AuthMethod	Comments

Enter your IPSec tunnel settings.
Under Name enter “IPSec-tunnel”.
Under Local Network select “lannet” (this is the private network on this side of the VPN tunnel).
Under Remote Network select “VPN-Remote-LAN” (this is the private network on the other side of the VPN tunnel, see **Step 2**).
Under Remote Endpoint select “VPN-Remote-IP” (this is the public up of the remote network, see **Step 3**).
Encapsulation Mode should be set to Tunnel.
Under Algorithms select the desired algorithms and IKE/IPSec lifetime. In our example we are using “Medium” settings.
You can modify or add your own set of security algorithms under Objects > VPN Objects > IKE Algorithms and IPSec Algorithms.



IPsec Tunnel

General

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

Name: IPSec-tunnel
Local Network: lannet
Remote Network: VPN-Remote-LAN
Remote Endpoint: VPN-Remote-IP

Encapsulation Mode: Tunnel

Algorithms

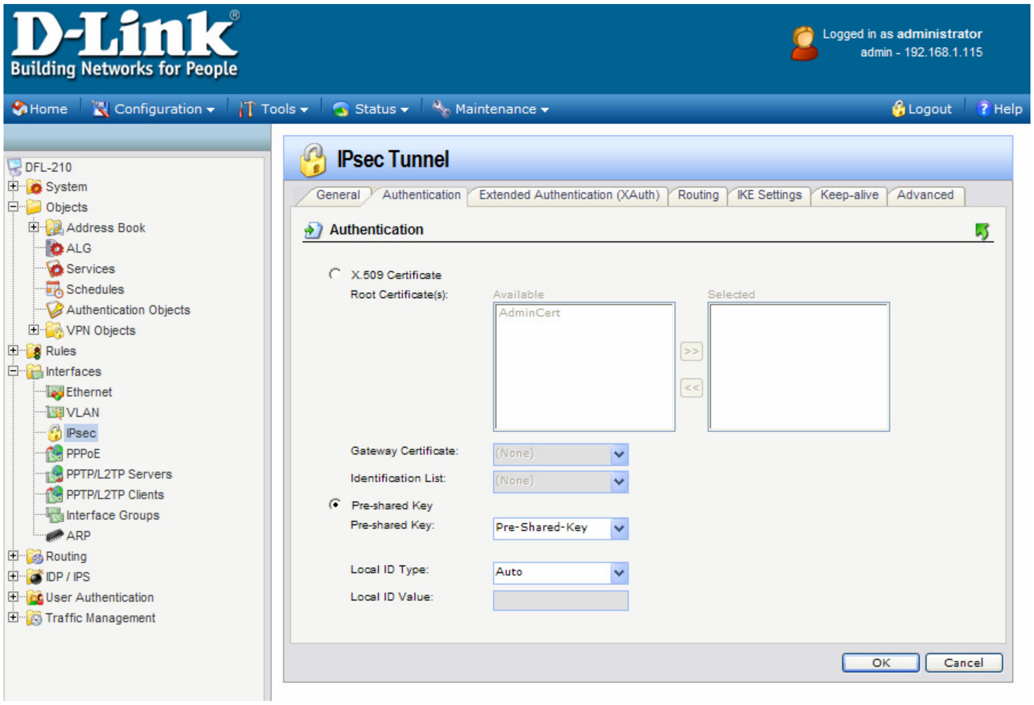
IKE Algorithms: Medium
IKE Life Time 28800 seconds

IPsec Algorithms: Medium
IPsec Life Time 3600 seconds
IPsec Life Time 0 kilobytes

Comments

Comments:

Click on Authentication tab. Make sure the Pre-Shared Key option is enabled. Select the “Pre-Shared-Key” in the dropdown menu (see **Step 4**).
Click on the OK button.

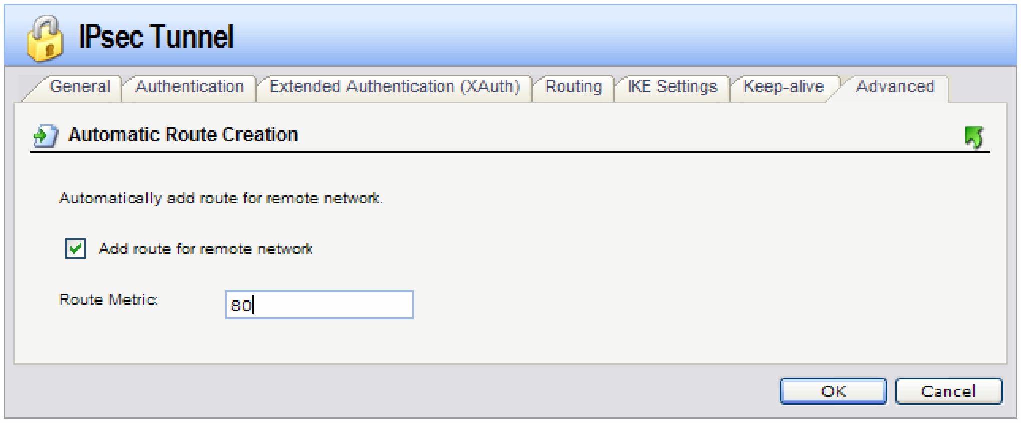


IPsec Tunnel

Authentication

○ X.509 Certificate
Root Certificate(s): Available: AdminCert Selected:
Gateway Certificate: (None)
Identification List: (None)
● Pre-shared Key
Pre-shared Key: Pre-Shared-Key
Local ID Type: Auto
Local ID Value:

If the WAN port of the firewall is set with PPPoE authentication, select Advanced tab and change the Route Metric for the IPSec Tunnel to 80.



IPsec Tunnel

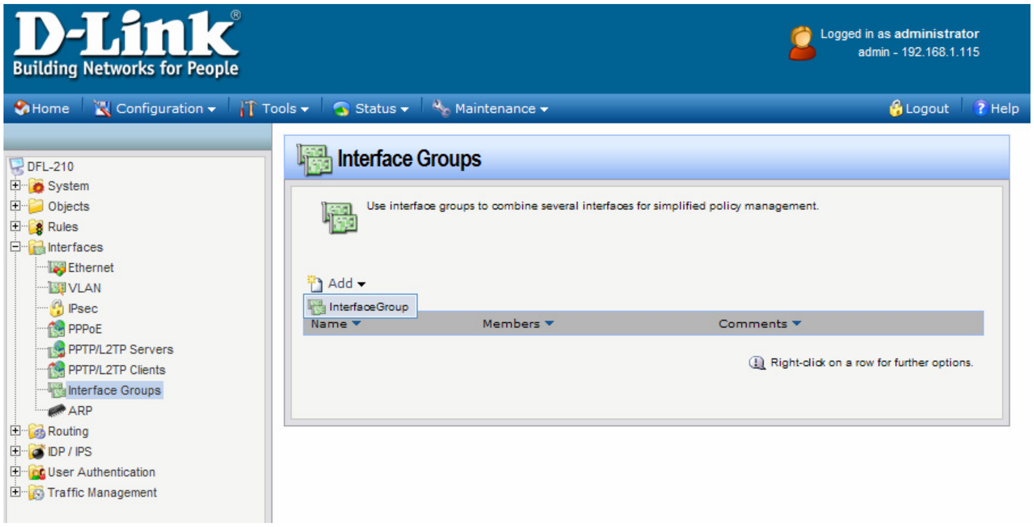
Automatic Route Creation

Automatically add route for remote network.

☑ Add route for remote network

Route Metric: 80

Step 6. Go to Interfaces > Interface Groups. Click on Add and select Interface Group.

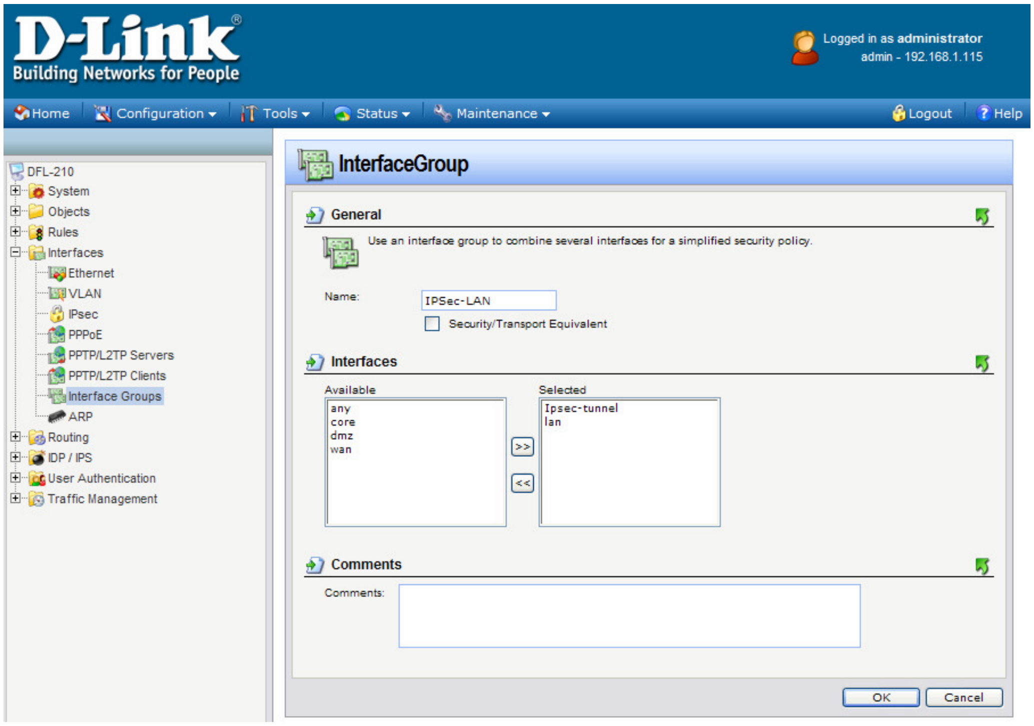


Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

Name	Members	Comments

Create a group which has your IPSec tunnel and your LAN.
Under Name type IPSec-LAN.
Under Interfaces add "IPSec-tunnel" and "lan" into Selected field.
Click on the OK button.



InterfaceGroup

General

Use an interface group to combine several interfaces for a simplified security policy.

Name: IPSec-LAN

□ Security/Transport Equivalent

Interfaces

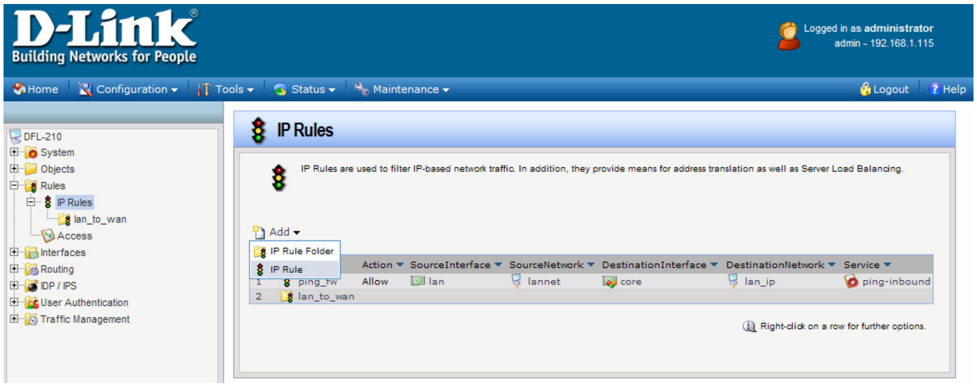
Available: any, core, dmz, wan

Selected: Ipsec-tunnel, lan

Comments

Comments:

Step 7. Go to Rules > IP Rules. Click on Add and select IP Rule.



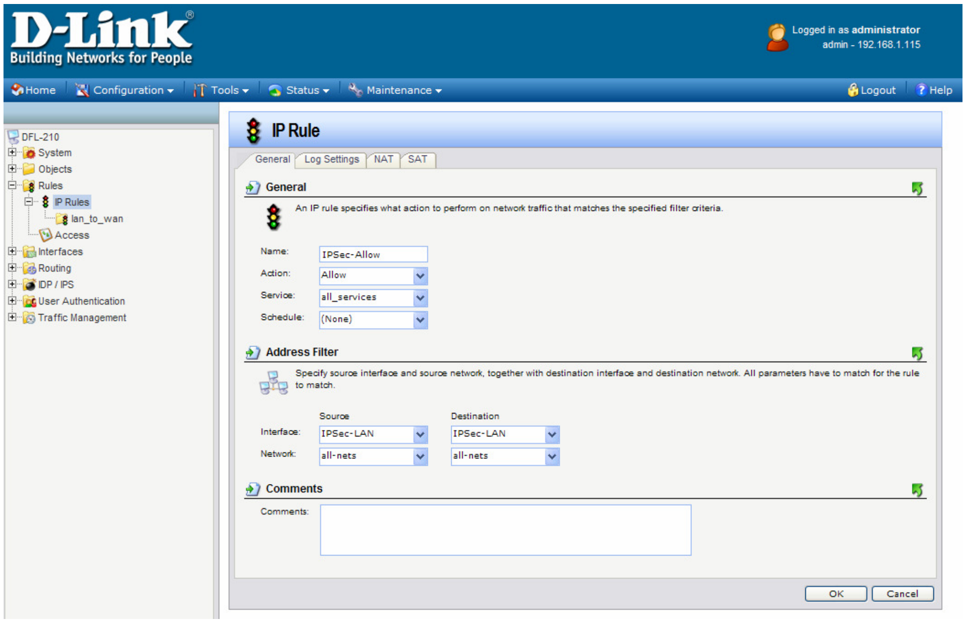
IP Rules

IP Rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

		Action	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
1	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
2	lan_to_wan						

Right-click on a row for further options.

This rule will allow communication between the LAN and the IPSec tunnel.
Under Name type “IPSec-Allow”.
Under Action select “Allow”.
Under Service select “all_services”.
Under Address Filter specify the following:
Source and Destination Interfaces: “IPSec-LAN” (this is the group you created in **Step 6**).
Source and Destination Network: select “all-nets”.



IP Rule

General

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

Name: IPSec-Allow
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

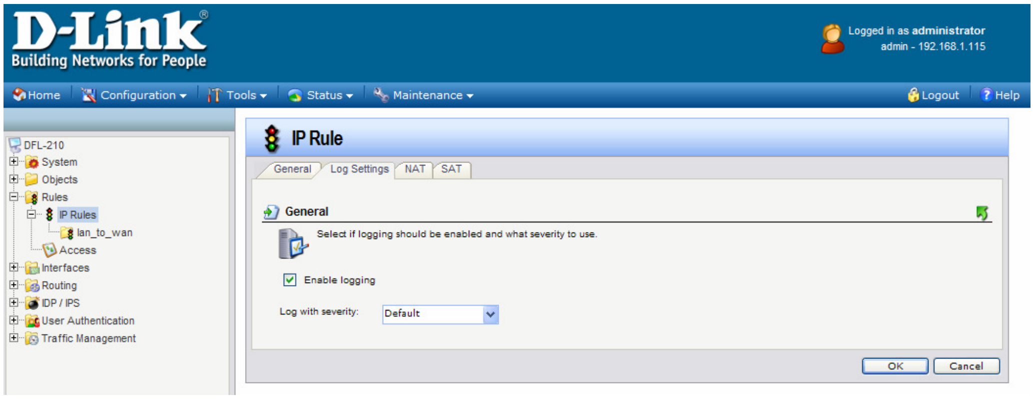
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	IPSec-LAN	IPSec-LAN
Network:	all-nets	all-nets

Comments

Comments:

Click on Log Settings tab.
Select the Enable Logging option.
Click on the OK button when done.



IP Rule

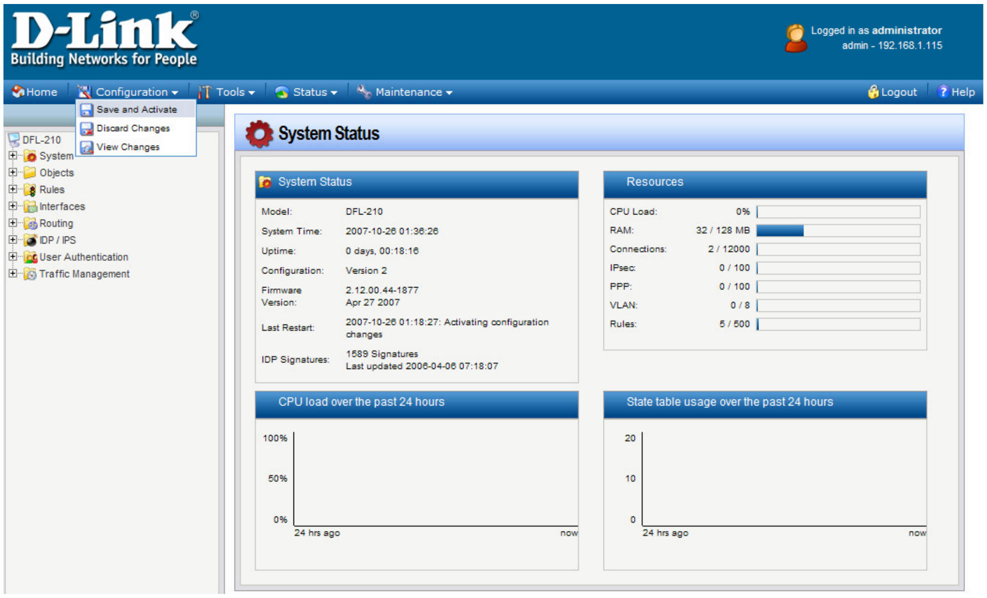
General

Select if logging should be enabled and what severity to use.

☑ Enable logging

Log with severity: Default

Step 8. Save the new configuration. In the top menu bar click on Configuration and select "Save and Activate".



System Status

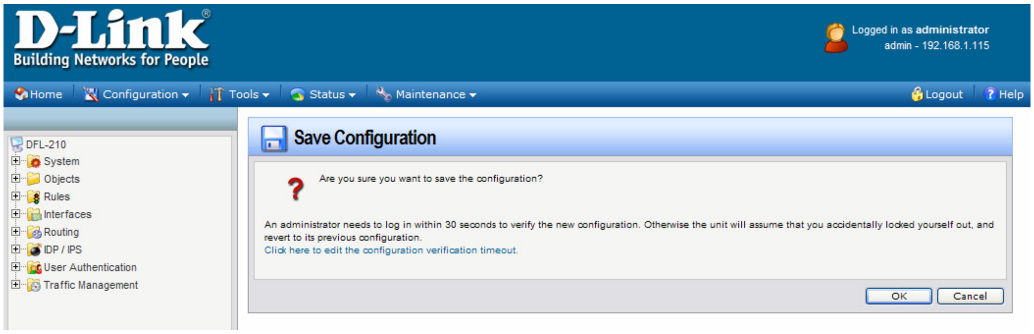
System Status

Model:	DFL-210
System Time:	2007-10-26 01:36:26
Uptime:	0 days, 00:18:16
Configuration:	Version 2
Firmware Version:	2.12.00.44-1877 Apr 27 2007
Last Restart:	2007-10-26 01:18:27: Activating configuration changes
IDP Signatures:	1589 Signatures Last updated 2006-04-06 07:18:07

Resources

CPU Load:	0%
RAM:	32 / 128 MB
Connections:	2 / 12000
IPsec:	0 / 100
PPP:	0 / 100
VLAN:	0 / 8
Rules:	5 / 500

Click on OK to confirm the new settings activation:



Save Configuration

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.
Click here to edit the configuration verification timeout.

Wait 15 seconds for the Firewall to apply the new settings.

Configuration of the Firewall on LAN 2

The steps to configure the second firewall will be almost identical to the steps for the firewall on the LAN 1. The only exception is the “Remote Network” and the “Remote Endpoint” settings. Note that the subnets on each LAN connecting through VPN should be different.

Step 1. Log into the Firewall on LAN 2. In our example we are using 192.168.0.1 address. Enter Username and Password which you specified during the initial setup of the Firewall.

Step 2. Go to Objects > Address Book > Interface Addresses. Click on Add and select “IP4 Host/Network”.
Specify the settings of the remote network on the other end of the VPN tunnel.
Under Name enter “VPN-Remote-LAN”.
Under IP Address enter the Subnet ID and Mask Bits for the remote network: in our example it is 192.168.1.0/24. Click on the OK button.

Step 3. Add another “IP4 Host/Network”. Enter the settings of the VPN endpoint, the public IP address of LAN 1.
Under Name type “VPN-Remote-IP”.
Under IP address specify the public IP address of the remote network (the IP address assigned by the ISP).

Step 4. Go to Object > VPN Objects > Pre-Shared Keys. Click on Add and select Pre-Shared Key.
Enter the Pre-Shared Key settings for your VPN tunnel.
Under Name type “Pre-Shared-Key”.
Under Shared Secret select the type of key you want to use and type in the key. In our example we are using ASCII key (passphrase). Note that it should be exactly the same key you set up on the LAN 1 firewall. Click OK when done.

Step 5. Go to Interfaces > IPSec Tunnels. Click on Add and select IPSec Tunnel.
Enter your IPSec tunnel settings.
Under Name enter “IPSec-tunnel”.
Under Local Network select “lannet” (this is the private network on this side of the VPN tunnel).
Under Remote Network select “VPN-Remote-LAN” (this is the private network on the other side of the VPN tunnel, see Step 2).
Under Remote Endpoint select “VPN-Remote-IP” (this is the public up of the remote network, see Step 3).
Encapsulation Mode should be set to Tunnel.
Under Algorithms select the desired algorithms and IKE/IPSec lifetime. The settings should correspond with the settings on the remote VPN Firewall.
Click on Authentication tab. Make sure the Pre-Shared Key option is enabled. Select the “Pre-Shared-Key” in the dropdown menu (see Step 4). Click on the OK button.

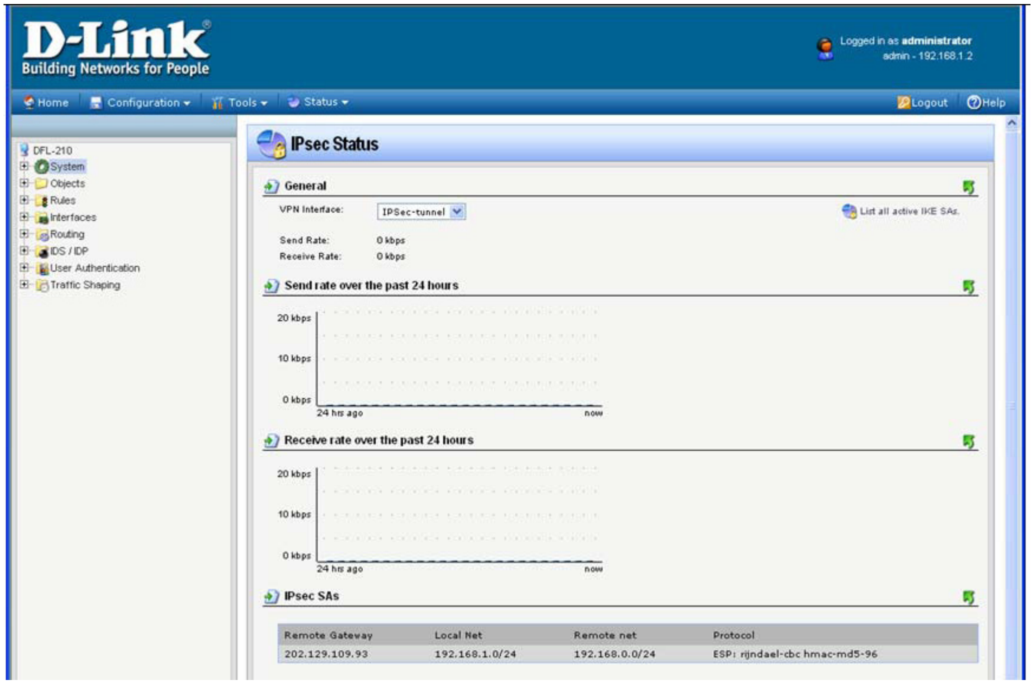
Step 6. Go to Interfaces > Interface Groups. Click on Add and select Interface Group.
Create a group which has your IPSec tunnel and your LAN.
Under Name type IPSec-LAN.
Under Interfaces add “IPSec-tunnel” and “lan” into Selected field. Click on the OK button.

Step 7. Go to Rules > IP Rules. Click on Add and select IP Rule.
This rule will allow communication between the LAN and the IPSec tunnel.
Under Name type “IPSec-Allow”.
Under Action select “Allow”.
Under Service select “all_services”.
Under Address Filter specify the following:
Source and Destination Interfaces: “IPSec-LAN” (this is the group you created in Step 6).
Source and Destination Network: select “all-nets”.
Click on Log Settings tab.
Select the Enable Logging option.
Click on the OK button when done.

Step 8. Save the new configuration. In the top menu bar click on Configuration and select “Save and Activate”. Click on OK to confirm the new settings activation.
Wait 15 seconds for the Firewall to apply the new settings.

Connecting via VPN tunnel

To check the status of your VPN connection, click on Status and select IPSec. If the VPN tunnel is up, you will see an active entry under IPSec SAs.



IPsec Status

General

VPN Interface: IPSec-tunnel

Send Rate: 0 kbps
Receive Rate: 0 kbps

Send rate over the past 24 hours

Receive rate over the past 24 hours

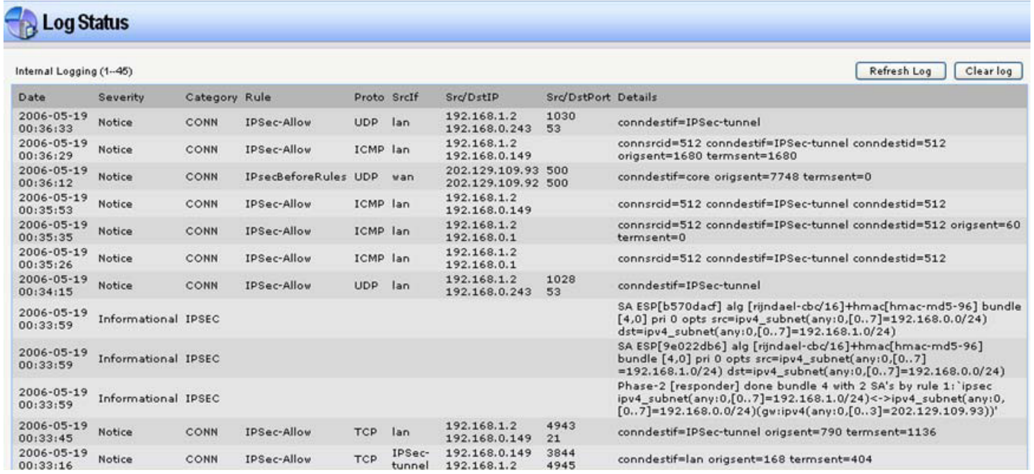
IPsec SAs

Remote Gateway	Local Net	Remote net	Protocol
202.129.109.93	192.168.1.0/24	192.168.0.0/24	ESP: rijndael-cbc hmac-md5-96

In order to trigger the VPN firewall to establish VPN tunnel try accessing any IP address on the remote private network (e.g. ping an IP address on remote LAN).

If VPN Tunnel can not be established:
- Make sure that the modems in front of the firewalls support VPN passthrough.
- Check the Pre-shared keys, security algorithms and life times, make sure they match on both VPN firewalls.
- Restart both firewalls.

You can see the connection log under Status > Logging.

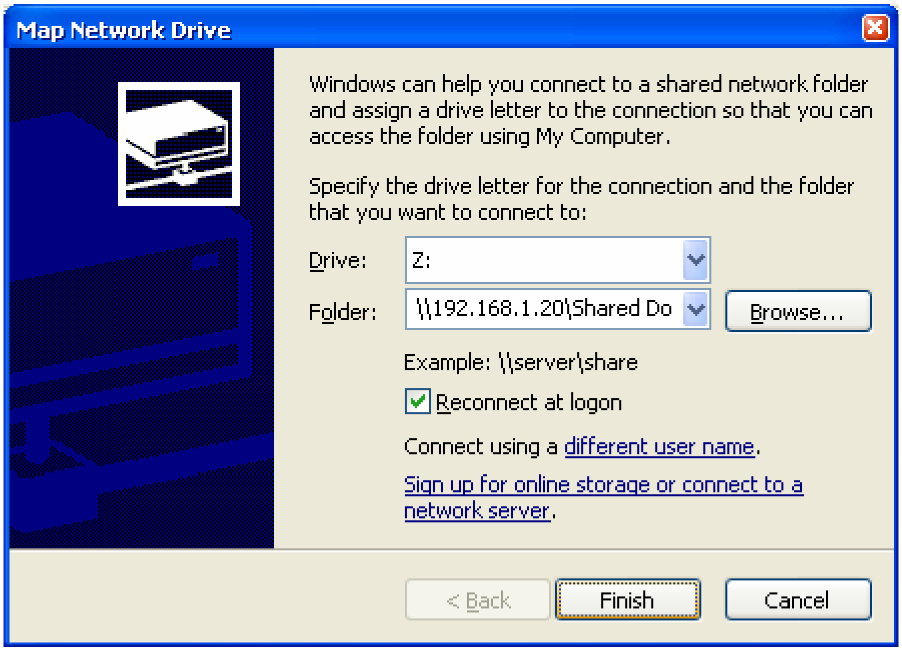


Log Status

Internal Logging (1--45)

Date	Severity	Category	Rule	Proto	SrcIf	Src/DstIP	Src/DstPort	Details
2006-05-19 00:36:33	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2 192.168.0.243	1030 53	conndestif=IPSec-tunnel
2006-05-19 00:36:29	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2 192.168.0.149		connsrcid=512 conndestif=IPSec-tunnel conndestid=512 origsent=1680 termsent=1680
2006-05-19 00:36:12	Notice	CONN	IPsecBeforeRules	UDP	wan	202.129.109.93 202.129.109.92	500 500	conndestif=core origsent=7748 termsent=0
2006-05-19 00:35:53	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2 192.168.0.149		connsrcid=512 conndestif=IPSec-tunnel conndestid=512
2006-05-19 00:35:35	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2 192.168.0.1		connsrcid=512 conndestif=IPSec-tunnel conndestid=512 origsent=60 termsent=0
2006-05-19 00:35:26	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2 192.168.0.1		connsrcid=512 conndestif=IPSec-tunnel conndestid=512
2006-05-19 00:34:15	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2 192.168.0.243	1028 53	conndestif=IPSec-tunnel
2006-05-19 00:33:59	Informational	IPSEC						SA ESP[b570dacf] alg [rijndael-cbc/16]+hmac[hmac-md5-96] bundle [4,0] pri 0 opts src=ipv4_subnet(any:0,[0..7]=192.168.0.0/24) dst=ipv4_subnet(any:0,[0..7]=192.168.1.0/24)
2006-05-19 00:33:59	Informational	IPSEC						SA ESP[9e022db6] alg [rijndael-cbc/16]+hmac[hmac-md5-96] bundle [4,0] pri 0 opts src=ipv4_subnet(any:0,[0..7] =192.168.1.0/24) dst=ipv4_subnet(any:0,[0..7]=192.168.0.0/24)
2006-05-19 00:33:59	Informational	IPSEC						Phase-2 [responder] done bundle 4 with 2 SA's by rule 1:`ipsec ipv4_subnet(any:0,[0..7]=192.168.1.0/24)<->ipv4_subnet(any:0,[0..7]=192.168.0.0/24)(gw:ipv4(any:0,[0..3]=202.129.109.93))'
2006-05-19 00:33:45	Notice	CONN	IPSec-Allow	TCP	lan	192.168.1.2 192.168.0.149	4943 21	conndestif=IPSec-tunnel origsent=790 termsent=1136
2006-05-19 00:33:16	Notice	CONN	IPSec-Allow	TCP	IPSec- tunnel	192.168.0.149 192.168.1.2	3844 4945	conndestif=lan origsent=168 termsent=404

To connect to shared resources via VPN you can map remote computers' drives and folders by opening Windows Explorer and going to Tools > Map Network Drive (you need to specify the IP address of the computer on remote network and the name of the shared folder):



Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.20\Shared Do

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

Alternatively you can do Search > Computers or People > Computer on Network > specify the IP address of the computer you are trying to connect to.
If you do not see computers in My Network Places or My Network Neighbourhood you may need to enable NetBIOS over TCP/IP in Windows.
Note that firewall/antivirus software installed on your or remote computer may stop you from accessing remote network.