

Interoperability Profiles for D-Link

DFL-260

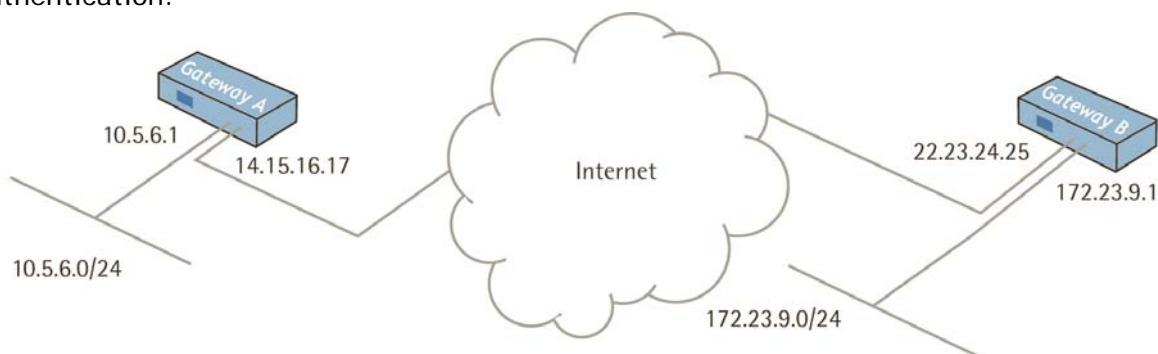
Last update: 2007-11-01

Overview

This document describes how to configure the D-Link DFL-260 firewall to implement scenario 1, specified in "Documentation Profiles for IPsec interoperability" by the VPN Consortium.

Scenario 1: Gateway-to-gateway with pre-shared secrets

The following is a typical gateway-to-gateway VPN that uses a pre-shared secret for authentication.



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:

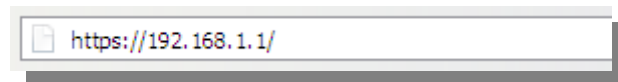
- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, follow these steps:

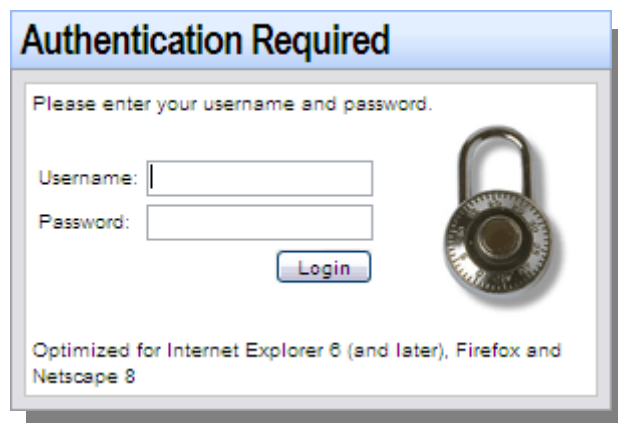
Configuring D-Link DFL-260

The default IP address for the **lan** interface on the DFL-260 is **192.168.1.1**. Connect your PC to the **lan** interface and use Internet Explorer 7.0+, Firefox 2.0+ or Opera 9.0+ to set up the DFL. In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** should first be clicked (expanded) and then **Address Book**.

In the web browser, connect to the firewall's web user interface using the address **https://192.168.1.1**



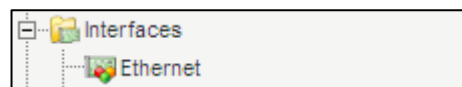
When you are connected to the DFL-260 you will need to log in. The default administrator username is **admin** and password **admin**.



1. Setting up the addresses and networks

Go to *Interfaces* -> *Ethernet*:

Click on the **wan** interface.
Uncheck the **Enable DHCP Client** checkbox.
Click **Ok**.



Go to *Objects* -> *Address book* -> *InterfaceAddresses*:

Edit the following items:
Change **lan_ip** to **10.5.6.1**
Change **lanet** to **10.5.6.0/24**
Change **wan_ip** to **14.15.16.17**
Change **wanet** to **14.16.17.0/24**

A screenshot of the 'InterfaceAddresses' configuration page. The page title is 'InterfaceAddresses'. Below the title, there is a message: 'Use an Address Folder to group related address objects for a better overview.' Below this message is an 'Add' button with a dropdown arrow. Below the button is a table with 8 rows and 3 columns: '#', 'Name', and 'Address'. The table contains the following data:

#	Name	Address
0	lan_ip	10.5.6.1
1	lanet	10.5.6.0/24
2	dmz_ip	172.17.100.254
3	dmznet	172.17.100.0/24
4	wan1_ip	14.15.16.17
5	wan1net	14.15.16.0/24
6	wan2_ip	192.168.120.254
7	wan2net	192.168.120.0/24

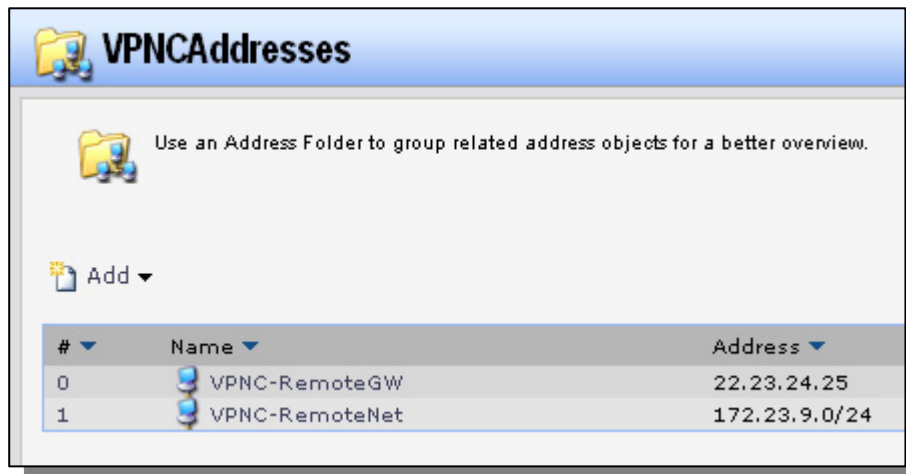
Go to *Objects* -> *Address book*:

Add a new Address Folder named **VPNAddresses**.

In the new folder, create the following objects:

Add an IP Address object called **VPN-RemoteGW** with the address **22.23.24.25**

Add an IP Address object called **VPN-RemoteNet** with the address **172.23.9.0/24**



2. Setting up required VPN objects

Go to *Objects* -> Authentication Objects:

Add a new Pre-Shared Key

Enter Name: **VPNC-PSK**

Select **Passphrase**

Enter **hr5xb8416aa9r6** as Shared Secret and confirm the pass phrase in the Confirm Secret box

Click **Ok**

Go to *Objects* -> *VPN Objects* -> *IKE Algorithms*:

Add a new IKE algorithm

Enter Name: **VPNC-IKE**

	Preferred	Min	Max
<input type="checkbox"/> Null			
<input type="checkbox"/> DES	64	64	64
<input checked="" type="checkbox"/> 3DES	192	192	192
<input type="checkbox"/> CAST128	128	128	128

Select **3DES**

MD5: <input type="checkbox"/>	SHA1: <input checked="" type="checkbox"/>
-------------------------------	---

Select **SHA1**

Click **Ok**

Go to *Objects* -> *VPN Objects* -> *IPsec Algorithms*:

Add a new IPsec algorithm

Enter Name: **VPNC-IPsec**

Select **3DES**

Select **SHA1**

Click **Ok**

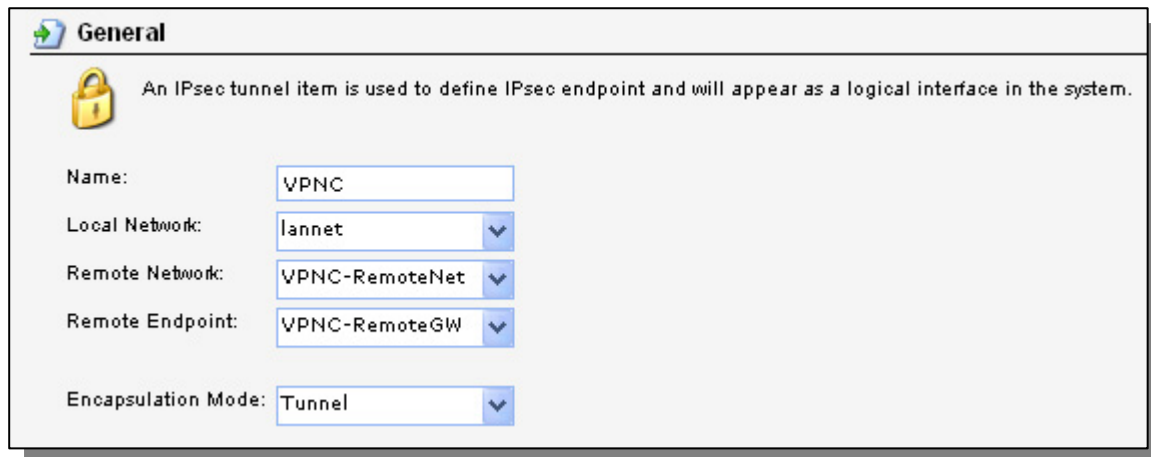
3. Setting up the IPsec tunnel

Go to *Interfaces* - > *IPsec*:

Add a new IPsec Tunnel

In the General tab:

General:



The screenshot shows the 'General' configuration tab for an IPsec tunnel. At the top, there is a lock icon and a note: 'An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.' Below this, several configuration fields are visible: 'Name' is set to 'VPNC'; 'Local Network' is a dropdown menu set to 'lannet'; 'Remote Network' is a dropdown menu set to 'VPNC-RemoteNet'; 'Remote Endpoint' is a dropdown menu set to 'VPNC-RemoteGW'; and 'Encapsulation Mode' is a dropdown menu set to 'Tunnel'.

Enter Name: **VPNC**

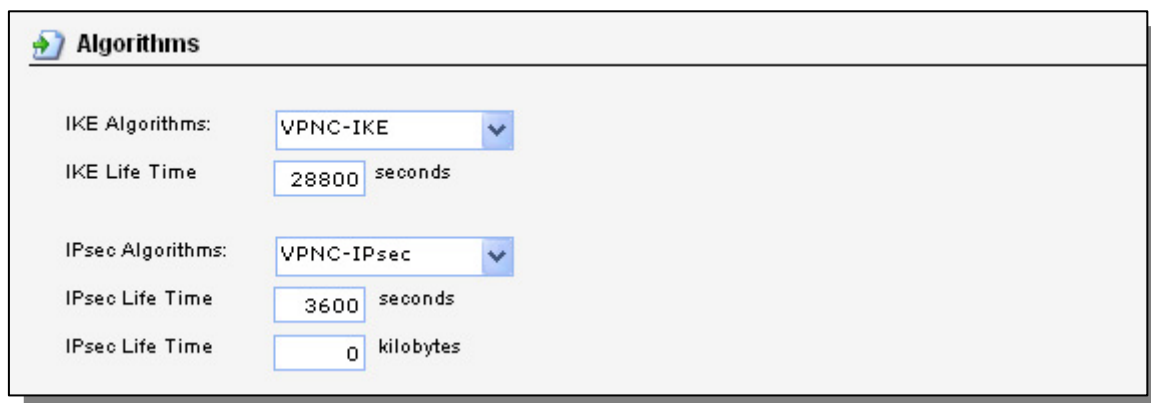
Select Local Network: **lannet**

Select Remote Network: **VPNC-RemoteNet**

Select Remote Endpoint: **VPNC-RemoteGW**

Select Encapsulation Mode: **Tunnel**

Algorithms:



The screenshot shows the 'Algorithms' configuration tab for the IPsec tunnel. It contains several fields: 'IKE Algorithms' is a dropdown menu set to 'VPNC-IKE'; 'IKE Life Time' is a text input field containing '28800' followed by 'seconds'; 'IPsec Algorithms' is a dropdown menu set to 'VPNC-IPsec'; 'IPsec Life Time' is a text input field containing '3600' followed by 'seconds'; and another 'IPsec Life Time' is a text input field containing '0' followed by 'kilobytes'.

Select IKE Algorithms: **VPNC-IKE**

Enter IKE Life Time: **28800** seconds

Select IPsec Algorithms: **VPNC-IPsec**

Enter IPsec Life Time: **3600** seconds

Enter IPsec Life Time: **0** kilobytes

Change to the Authentication tab:

Authentication:



Pre-Shared Key
Pre-Shared Key:

Select Pre-Shared key and **VPNC-PSK**

Change to the IKE Settings tab:

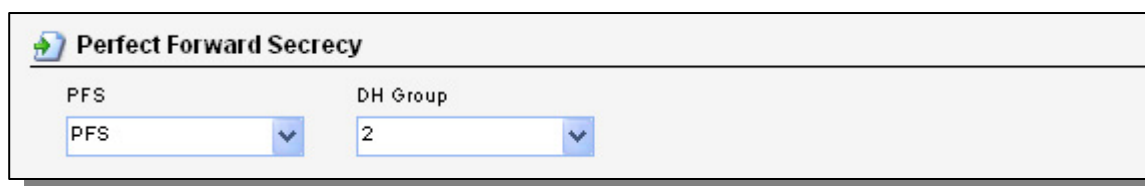
IKE:




 **IKE**
 Main DH Group
 Aggressive

Select Main and **DH Group 2**

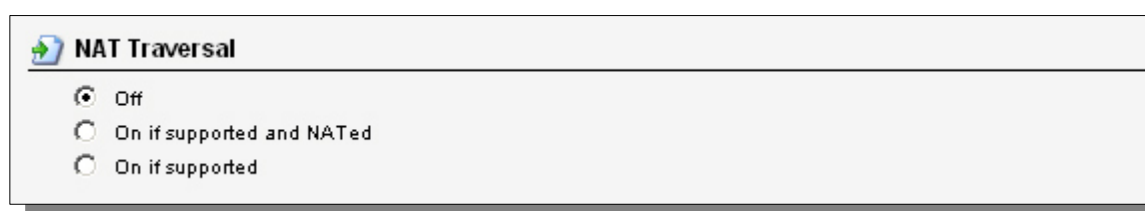
Perfect Forward Secrecy:



 **Perfect Forward Secrecy**
PFS DH Group

Select **PSF** and **DH Group 2**

NAT Traversal:



 **NAT Traversal**
 Off
 On if supported and NATed
 On if supported

Select Nat Traversal: **OFF**

Click **Ok**.

4. Setting up rules

Go to *Rules* -> *IP Rules*:

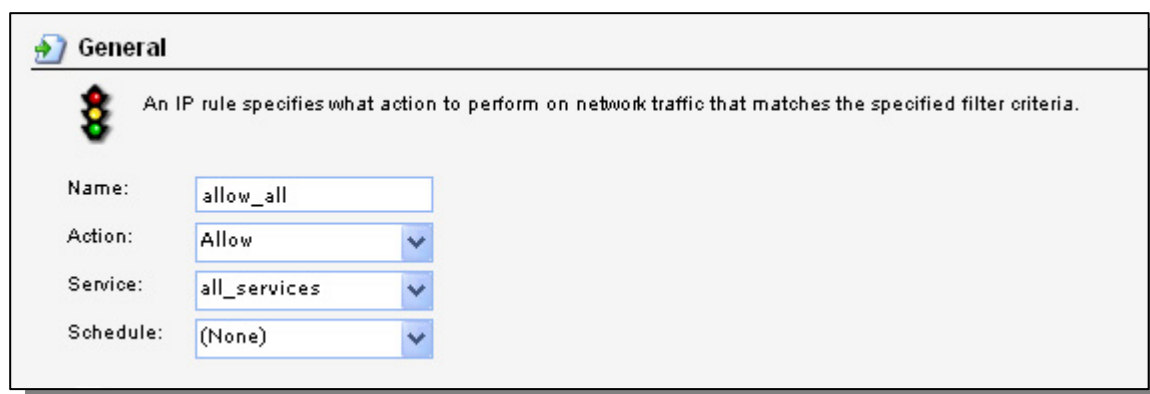
Add a new IP Rule Folder named **lan_to_VPNC**

In the new folder, create two rules

Add a new IP Rule

In the General tab:

General:



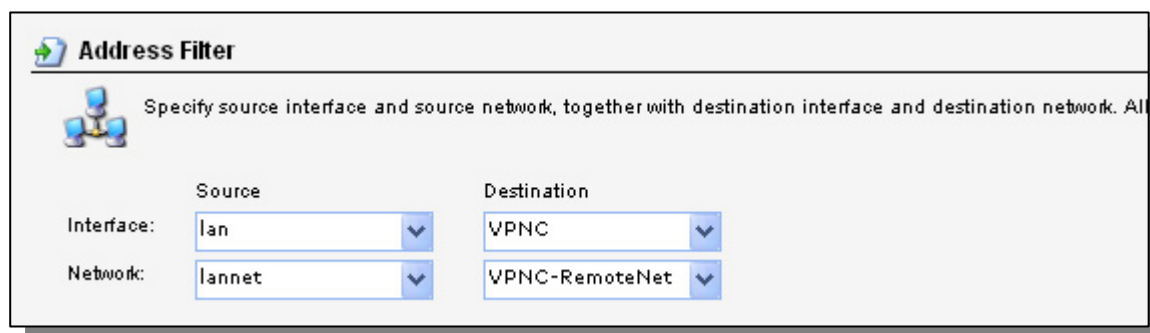
The screenshot shows the 'General' tab of an IP rule configuration window. At the top, there is a traffic light icon and a description: 'An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.' Below this, there are four fields: 'Name' with the value 'allow_all', 'Action' with a dropdown menu set to 'Allow', 'Service' with a dropdown menu set to 'all_services', and 'Schedule' with a dropdown menu set to '(None)'.

Enter Name: **allow_all**

Select Action: **allow**

Select Service: **all_services**

Address filter:



The screenshot shows the 'Address Filter' tab of an IP rule configuration window. At the top, there is a network icon and a description: 'Specify source interface and source network, together with destination interface and destination network. All'. Below this, there are four fields arranged in a 2x2 grid. The top row is labeled 'Interface' and the bottom row is labeled 'Network'. The left column is labeled 'Source' and the right column is labeled 'Destination'. The values are: Source Interface: 'lan', Source Network: 'lannet', Destination Interface: 'VPNC', and Destination Network: 'VPNC-RemoteNet'.

Select Source Interface: **lan**

Select Source Network: **lannet**

Select Destination Interface: **VPNC**

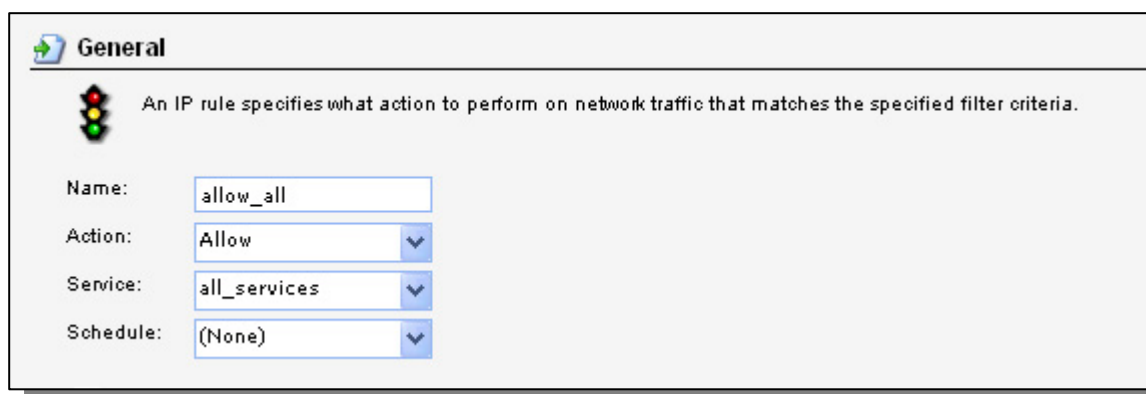
Select Destination Network: **VPNC-RemoteNet**

Click **OK**

Add a new IP Rule

In the General tab:

General:



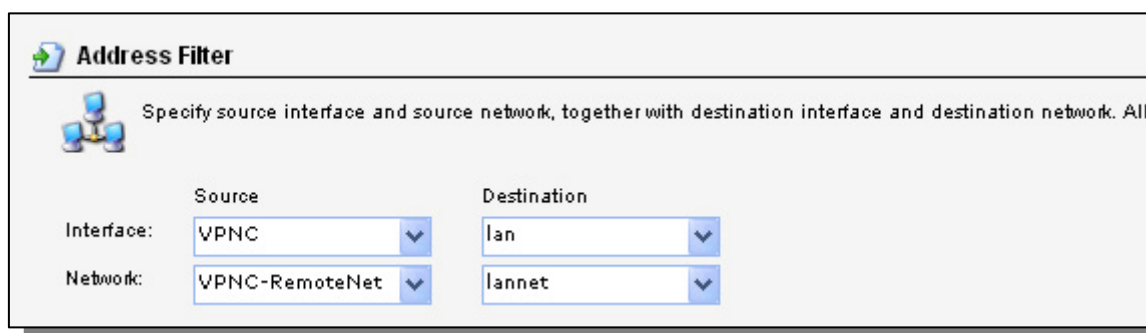
The screenshot shows the 'General' tab of an IP rule configuration window. At the top, there is a traffic light icon and a descriptive text: 'An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.' Below this, there are four configuration fields: 'Name' with the value 'allow_all', 'Action' with a dropdown menu set to 'Allow', 'Service' with a dropdown menu set to 'all_services', and 'Schedule' with a dropdown menu set to '(None)'.

Enter Name: **allow_all**

Select Action: **allow**

Select Service: **all_services**

Address filter:



The screenshot shows the 'Address Filter' tab of the IP rule configuration window. It features a network diagram icon and the text: 'Specify source interface and source network, together with destination interface and destination network. All'. Below this, there are four configuration fields arranged in a 2x2 grid. The top row is labeled 'Interface' and the bottom row is labeled 'Network'. The left column is labeled 'Source' and the right column is labeled 'Destination'. The values are: Source Interface: 'VPNC', Source Network: 'VPNC-RemoteNet', Destination Interface: 'lan', and Destination Network: 'lannet'.

Select Source Interface: **VPNC**

Select Source Network: **VPNC-RemoteNet**

Select Destination Interface: **lan**

Select Destination Network: **lannet**

Click **Ok**

Save and activate the new configuration.

5. Tools

Useful tools that can be used in the firewall are:

Ping:

Ping a remote gateway or computer to check connections, rules etc.

WebUI: Tools->Ping

Console: ping <ipaddress>, ping <ipaddress> -r <rcvif>, ping <ipaddress> -s <srcip>

Kill active SA:

Can be used to disconnect already established tunnels.

WebUI: Status->IPsec->List all active SAs

Console: killsa <ipaddress>

6. Status

The following pages in the WebUI or commands in the console can be used to view the status of the setup or find problems.

Interface status:

Can be used to view IP addresses of the interfaces, link status, hardware addresses and more.

WebUI: Status->Interfaces

Console: ifstat <interfacename>

IPsec status:

Can be used to see the settings of the IPsec tunnel, if the tunnel is established and other useful information.

WebUI: Status->IPsec

Console: ipsecstat, ipsecstat -u, ipsecstat -v, ipsecconn

IKE snooping:

Can be used to find problems in the IKE negotiations.

Console: ikesnoop on, ikesnoop verbose, ikesnoop off

Logging:

Can be used to find a lot of useful information, eg if traffic is dropped.

WebUI: Status->Logging

Connections:

Can be used to see the current connections in the firewall.

WebUI: Status->Connections

Console: connections

