

How to configure policies in the DFL-600

Example:

- Allow port redirection on port 80 TCP for ANY IP address (anyone can see the web site)
- Allow port redirection on port 3389 TCP for certain IP address only, e.g. 201.2.2.2 (only 201.2.2.2 can use Remote Desktop connection).

1. Add two virtual servers to redirect TCP port 80 and 3389 to internal servers.

D-Link
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

Home Advanced Tools Status Help

Virtual Server / Application(ALG)

Add Virtual Server Mapping

Private IP address: 192.168.0.101

Transport Type: TCP

Protocol: --user defined--

Port Number: 3389

Apply Cancel Help

Total No. of Entries: 2 / 8

Private IP address	Protocol Type	Port Number	Delete
192.168.0.102	TCP	80	
192.168.0.101	TCP	3389	

Page 1

2. After adding 2 virtual servers as above, add two policy rules as below:

Policy Rules / [Global Policy Status](#) / [Policies](#)
[Rule Add](#) / [Domain Add](#) / [MAC Add](#) / [Keywords Add](#)

Rule Name:
 Transport Type:
 Protocol:
 Direction:
 Port Range: ☐ Any - (1 - 65535)
 Source IP Range: ☐ Any -
 Destination IP Range: ☐ Any -

Service Rules

Total No. of Entries(In+Out / Total): 2 / 1000

Rule name	Type	Protocol	Source ip	Destination ip	Dir.	View	Del
VS-80	TCP	80 - 80	*	192.168.0.102 192.168.0.102	in	View	Del
VS-3389	TCP	3389 - 3389	*	192.168.0.101 192.168.0.101	in	View	Del

Page 1

3. Edit these two rules. Press  in "View" field to edit these two rules to meet your requirements. For rule VS-80 (anyone can see the web site), Source IP range set to "ANY".

Policy Rules / [Global Policy Status](#) / [Policies](#)
[Rule Add](#) / [Domain Add](#) / [MAC Add](#) / [Keywords Add](#)

Rule Name:
 Transport Type:
 Protocol:
 Direction:
 Port Range: ☐ Any - (1 - 65535)
 Source IP Range: ☒ Any -
 Destination IP Range: ☐ Any -

Service Rules

Total No. of Entries(In+Out / Total): 2 / 1000

Rule name	Type	Protocol	Source ip	Destination ip	Dir.	View	Del
VS-80	TCP	80 - 80	*	192.168.0.102 192.168.0.102	in	View	Del
VS-3389	TCP	3389 - 3389	*	192.168.0.101 192.168.0.101	in	View	Del

Page 1

For rule VS-3389 (only 201.2.2.2 can use Remote Desktop connection), Source IP Range must have "201.2.2.2-201.2.2.2.

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

Policy Rules / [Global Policy Status](#) / [Policies](#)
Rule Add / [Domain Add](#) / [MAC Add](#) / [Keywords Add](#)

Rule Name: VS-3389
Transport Type: TCP
Protocol: --user defined--
Direction: Inbound
Port Range: ☐ Any 3389 - 3389 (1 - 65535)
Source IP Range: ☐ Any 201.2.2.2 - 201.2.2.2
Destination IP Range: ☐ Any 192.168.0.101 - 192.168.0.101

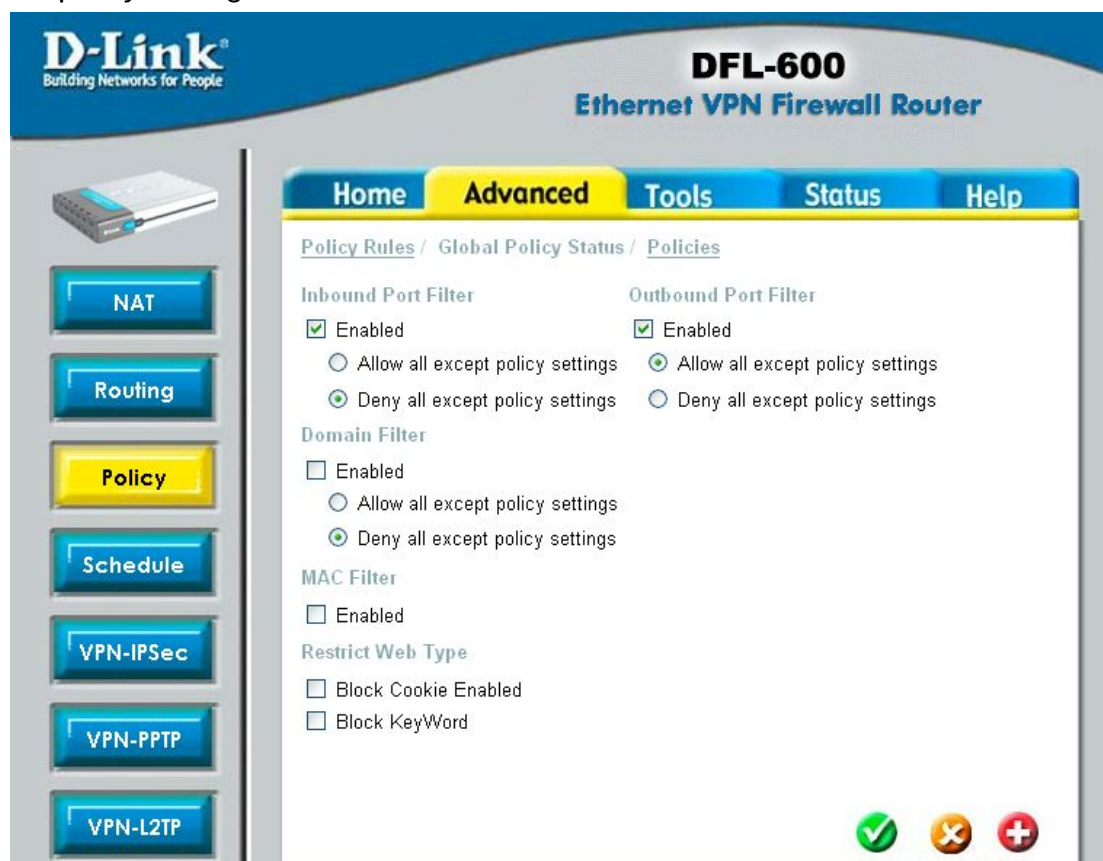
Apply **Cancel** **Help**

Service Rules Total No. of Entries(In+Out / Total): 2 / 1000

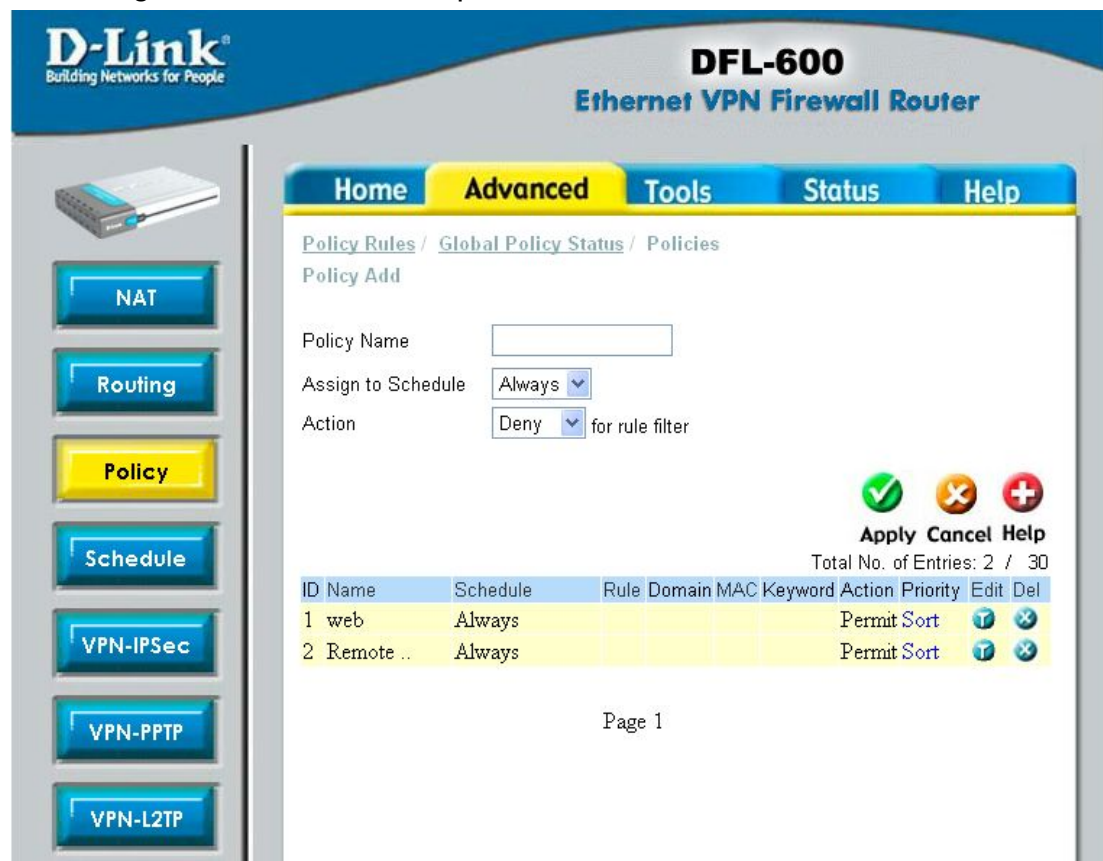
Rule name	Type	Protocol	Source ip	Destination ip	Dir.	View	Del
VS-80	TCP	80 - 80	*	192.168.0.102 192.168.0.102	in		
VS-3389	TCP	3389 - 3389	201.2.2.2 201.2.2.2	192.168.0.101 192.168.0.101	in		

Page 1

4. Configure "Global Policy Status" as below. In Inbound Port Filter enable "Deny all except policy settings".



5. Configure Policies. Add two policies as below:



5-1. Edit "web" policy.

Ethernet VPN Firewall Router

Home **Advanced** Tools Status Help

[Policy Rules](#) / [Global Policy Status](#) / [Policies](#)

Policy Name:

Assign to Schedule:

Action: for rule filter

Rule Filter

☐ Enabled

["Inbound Firewall Rule"](#) ["Outbound Firewall Rule"](#)

Domain Filter

☐ Enabled

["Allow Domain"](#)

MAC Filter

☐ Enabled

["Deny Blocked MAC"](#)

Keyword Filter

☐ Enabled

["Keywords Block"](#)

Apply Back Cancel Help

Go to "Inbound Firewall Rule" to choose rules.

D-Link
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

Home **Advanced** Tools Status Help

Grouping rules to Policy - web

Total No. of Entries: 2 / 1000

Add	ID	Rule Name	Type	Protocol	Source ip	Destination ip	Dir
☒	2	VS-80	TCP	80 - 80	*	192.168.0.102 192.168.0.102	in
☐	3	VS-3389	TCP	3389 - 3389	201.2.2.2 201.2.2.2	192.168.0.101 192.168.0.101	in

Page 1

Apply Back Cancel Help

Enable “Inbound Firewall Rule”.

Home **Advanced** Tools Status Help

Policy Rules / Global Policy Status / Policies

Policy Name:

Assign to Schedule:

Action: for rule filter

Rule Filter

☒ Enabled

"Inbound Firewall Rule" "Outbound Firewall Rule"

Domain Filter

☐ Enabled

"Allow Domain"

MAC Filter

☐ Enabled

"Deny Blocked MAC"

Keyword Filter

☐ Enabled

"Keywords Block"

☒ ☐ ☐ ☐

Apply Back Cancel Help

5-2. Edit Remote Desktop policy. Go to “Inbound Firewall Rule” to choose rules.

D-Link
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

Home **Advanced** Tools Status Help

Grouping rules to Policy - Remote Desktop

Total No. of Entries: 2 / 1000

Add	ID	Rule Name	Type	Protocol	Source ip	Destination ip	Dir
☐	2	VS-80	TCP	80 - 80	*	192.168.0.102 192.168.0.102	in
☒	3	VS-3389	TCP	3389 - 3389	201.2.2.2 201.2.2.2	192.168.0.101 192.168.0.101	in

Page 1

☒ ☐ ☐ ☐

Apply Back Cancel Help

Enable "Inbound Firewall Rule".

D-Link
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

Home **Advanced** Tools Status Help

[Policy Rules](#) / [Global Policy Status](#) / [Policies](#)

Policy Name: Remote Desktop

Assign to Schedule: Always

Action: Permit for rule filter

Rule Filter: ☒ Enabled

["Inbound Firewall Rule"](#) ["Outbound Firewall Rule"](#)

Domain Filter: ☐ Enabled

["Allow Domain"](#)

MAC Filter: ☐ Enabled

["Deny Blocked MAC"](#)

Keyword Filter: ☐ Enabled

["Keywords Block"](#)

6. You should see these two policies are enabled:

D-Link
Building Networks for People

DFL-600
Ethernet VPN Firewall Router

Home **Advanced** Tools Status Help

[Policy Rules](#) / [Global Policy Status](#) / [Policies](#)

Policy Add

Policy Name:

Assign to Schedule: Always

Action: Deny for rule filter

☒ ☐ ☐
 Apply Cancel Help

Total No. of Entries: 2 / 30

ID	Name	Schedule	Rule	Domain	MAC	Keyword	Action	Priority	Edit	Del
2	Remote ..	Always	Enable				Permit Sort			
1	web	Always	Enable				Permit Sort			

Page 1

~ End of Document ~