

# **NETDEFEND**

## Configuration examples for the D-Link NetDefend Firewall series

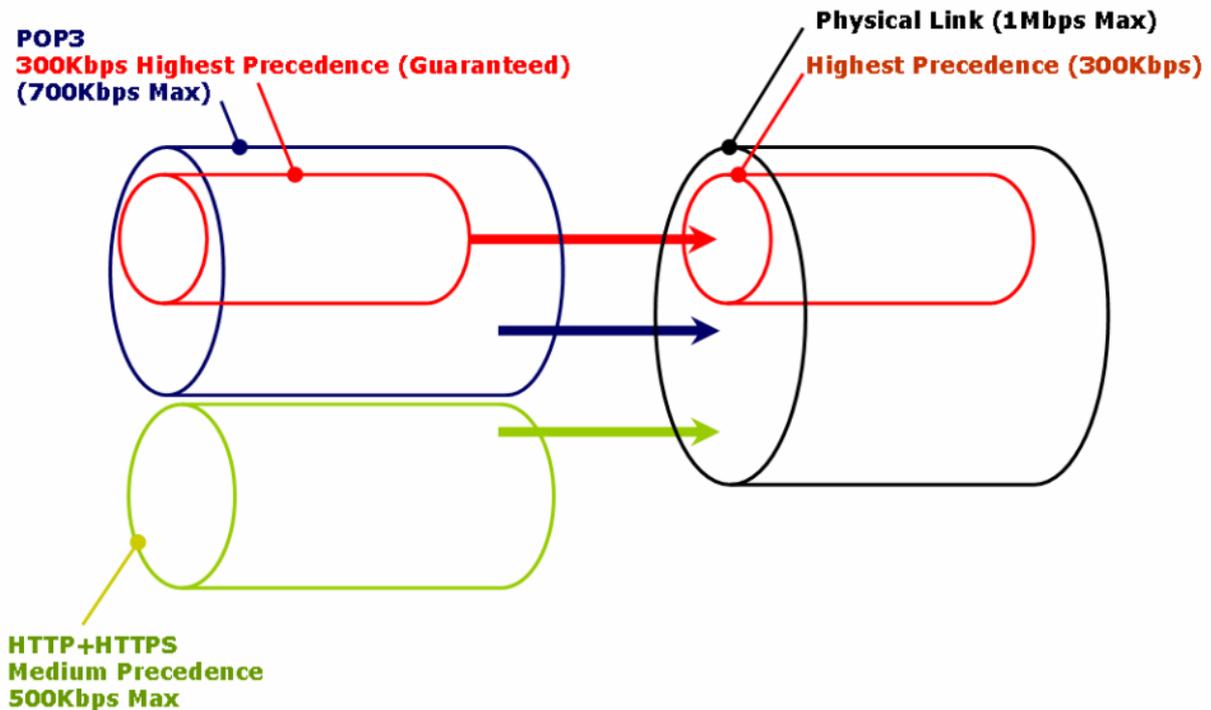


### How to setup traffic shaping

The below steps describe the configuration where we are using 1Mbps up / 1Mbps down link with the following traffic shaping rules:

- inbound and outbound HTTP and HTTPS the max bandwidth is 500Kbps.
- inbound and outbound POP3 the guaranteed bandwidth is 300Kbps, max is 700Kbps.
- other inbound and outbound services use the remaining bandwidth.

Here is the schematic representation of the three traffic shaping pipes we are going to create (we will need three pipes for outbound and three pipes for inbound traffic):



**Step 1.** Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is "admin" and password is "admin".

**Step 2.** Go to Policies > Traffic Management > Pipes.

Create a new entry for a “standard-in” pipe which describes physical connection limitations for download speed. Set the pipe limits: Total - 1000Kbps. Under Precedences set “7” with 300Kbps (this is for the guaranteed bandwidth).

Create another pipe for “standard-out” (upload speed). Set the pipe limits: Total - 1000Kb. Under Precedences set “7” with 300Kbps.

Policies » Traffic Management » Traffic Shaping » Pipes » wan1-std-in

## wan1-std-in

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

**General** | **Pipe Limits** | Group Limits

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

**i** Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second.
7:	<input type="text" value="300"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>
Total:	<input type="text" value="1000"/>	<input type="text"/>

**Step 3.** Create two pipes (in and out) for HTTP traffic: Total bandwidth – 500 kbps. Precedence: “4” with 500 kbps limit.

Policies » Traffic Management » Traffic Shaping » Pipes » http-in

### http-in

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

Policies » Traffic Management » Traffic Shaping » Pipes » http-out

### http-out

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

General   **Pipe Limits**   Group Limits

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

**i** Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:	Kilobits per second	Packets per second.
7:	<input type="text"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text" value="500"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>
Total:	<input type="text" value="500"/>	<input type="text"/>

**Step 4.** Create two more pipes (in and out) for POP3 traffic: Total bandwidth – 700 kbps. Precedence: “7” with 300 kbps limit.

Policies » Traffic Management » Traffic Shaping » Pipes » pop3-in

## pop3-in

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

Policies » Traffic Management » Traffic Shaping » Pipes » pop3-out

## pop3-out

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

Use pipe precedence  
precedence

General

Pipe Limits

Group Limits

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence.

**i** Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences: Kilobits per second      Packets per second.

7:	<input type="text" value="300"/>	<input type="text"/>
6:	<input type="text"/>	<input type="text"/>
5:	<input type="text"/>	<input type="text"/>
4:	<input type="text"/>	<input type="text"/>
3:	<input type="text"/>	<input type="text"/>
2:	<input type="text"/>	<input type="text"/>
1:	<input type="text"/>	<input type="text"/>
0:	<input type="text"/>	<input type="text"/>

Total:

**Step 5.** Go to Policies > Traffic Management > Pipe Rules. You need to create Pipe Rules which would direct the selected traffic (HTTP or POP3) into specific pipe.

Create a Pipe Rule for HTTP traffic. Service - HTTP-All; Source LAN/LAN-Net; Destination - WAN/All-nets. Click on Traffic Shaping tab and add the pipes for outgoing traffic (Forward Chain - HTTP-out, Standard-out) and incoming traffic (Return Chain - HTTP-in, Standard-in). Set Precedence to "4".

Policies » Traffic Management » Traffic Shaping » Pipe Rules » wan1-http

### wan1-http

A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

**General** | **Traffic Shaping**

Name: wan1-http 

Service: http-all 

Schedule: (None) 

---

**Address Filter**

Source: Interface: lan  Network: lannet 

Destination: wan1  all-nets 

**General** | **Traffic Shaping**

### Pipe Chains

Forward chain:

Available	Selected
http-in pop3-in pop3-out wan1-std-in	http-out wan1-std-out

+ Include      × Remove      ^      v

Return chain:

Available	Selected
http-out pop3-in pop3-out wan1-std-out	http-in wan1-std-in

+ Include      × Remove      ^      v

---

**Precedence**

Precedence: Use fixed 

Fixed Precedence: 4 

**Step 6.** Create a Pipe Rule for POP3 traffic. Service – POP3; Source LAN/LAN-Net; Destination - WAN/All-nets. Click on Traffic Shaping tab and add the pipes for outgoing traffic (Forward Chain – POP3-out, Standard-out) and incoming traffic (Return Chain – POP3-in, Standard-in). Set Precedence to “7”.

Policies » Traffic Management » Traffic Shaping » Pipe Rules » wan1-pop3

## wan1-pop3

A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

**General** **Traffic Shaping**

Name: wan1-pop3

Service: pop3

Schedule: (None)

**Address Filter**

Source: Interface: lan Network: lan-net

Destination: wan1 all-nets

**General** **Traffic Shaping**

### Pipe Chains

Forward chain:

Available	Selected
<ul style="list-style-type: none"> <li>http-in</li> <li>http-out</li> <li>pop3-in</li> <li>wan1-std-in</li> </ul>	<ul style="list-style-type: none"> <li>pop3-out</li> <li>wan1-std-out</li> </ul>
+ Include	× Remove

Return chain:

Available	Selected
<ul style="list-style-type: none"> <li>http-in</li> <li>http-out</li> <li>pop3-out</li> <li>wan1-std-out</li> </ul>	<ul style="list-style-type: none"> <li>pop3-in</li> <li>wan1-std-in</li> </ul>
+ Include	× Remove

**Precedence**

Precedence: Use fixed

Fixed Precedence: 7

**Step 7.** Create another Pipe Rule for the rest of the services. Click on Traffic Shaping tab and add the pipes for outgoing traffic (Forward Chain - Standard-out) and incoming traffic (Return Chain - Standard-in). Set Precedence to "0".

Policies » Traffic Management » Traffic Shaping » Pipe Rules » wan1-all

## wan1-all

A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

**General** | **Traffic Shaping**

Name: wan1-all 

Service:  all\_services ▼

Schedule: (None) ▼

---

**Address Filter**

Source: Interface: lan ▼ Network: lannet ▼

Destination: wan1 ▼ all-nets ▼

**General** | **Traffic Shaping**

### Pipe Chains

Forward chain:

Available	Selected
http-in http-out pop3-in pop3-out wan1-std-in	wan1-std-out

+ Include      × Remove      ▲ ▼

Return chain:

Available	Selected
http-in http-out pop3-in pop3-out wan1-std-out	wan1-std-in

+ Include      × Remove      ▲ ▼

---

**Precedence**

Precedence: Use fixed ▼

Fixed Precedence: 0 ▼

Make sure that the Pipe Rule for the rest of the traffic is positioned **after** the other rules.

Policies » Traffic Management » Traffic Shaping » Pipe Rules

## Pipe Rules

Define a traffic shaping policy by specifying what network traffic should flow through what pipes.

+ Add Filter:

# ^	Name	Source int...	Source ne...	Destinatio...	Destinatio...	Service	Comments
1	wan1-http	lan	lannet	wan1	all-nets	http-all	
2	wan1-pop3	lan	lannet	wan1	all-nets	pop3	
3	wan1-all	lan	lannet	wan1	all-nets	all_service:	

**Step 8.** Go to Policies > Firewalling > Main IP Rules > “lan\_to\_wan”. Create additional NAT rules for HTTP and POP3 traffic (you can “clone” the default “allow\_standard” NAT rule and change “all\_tcpudp” service to HTTP and POP3).

Make sure the new NAT rules are positioned above the “allow\_standard” NAT rule.

Policies » Firewalling » Rules » Main IP Rules » lan\_to\_wan1

## lan\_to\_wan1

An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

+ Add Edit this object

# ^	Name	L...	Src If	Src Net	Dest If	Dest Net	Service	Address Translation
1	drop_smb-all		lan	lannet	wan1	all-nets	smb-all	
2	allow_ping-outbound		lan	lannet	wan1	all-nets	ping-outbound	SRC:NAT
3	allow_ftp-passthrough		lan	lannet	wan1	all-nets	ftp-passthrough-av	SRC:NAT
4	POP3_NAT		lan	lannet	wan1	all-nets	pop3	SRC:NAT
5	HTTP_NAT		lan	lannet	wan1	all-nets	http-all	SRC:NAT
6	allow_standard		lan	lannet	wan1	all-nets	all_tcpudp	SRC:NAT

**Step 9.** After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

**NOTE:** If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.

