DMZ Configuration Example

This manual describes how to add DMZ hosts to a network.

Short for demilitarized zone, the term comes from military use, meaning a buffer area between two enemies. Applying it to IT sphere, it means computer or a small subnetwork that sits between a trusted internal network, such as corporate private LAN, and an untrusted external network, such as the public Internet.

Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP(e-mail) servers and DNS servers.

Consider the network diagram below:

The router should have 3 NIC cards:

```
[admin@gateway] interface> print
Flags: X - disabled, D - dynamic, R - running
  #  NAME     TYPE  RX-RATE  TX-RATE  MTU
  0  R Public  ether  0        0        1500
  1  R Local   ether  0        0        1500
  2  R DMZ-zone ether 0        0        1500

[admin@gateway] interface>
```

- Add all needed ip addresses to interfaces as is shown here:

```
[admin@gateway] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
  #  ADDRESS     NETWORK   BROADCAST INTERFACE
  0  192.168.0.2/24  192.168.0.0  192.168.0.255 Public
  1  10.0.0.254/24  10.0.0.0    10.0.0.255 Local
  2  10.1.0.1/32   10.1.0.0    10.1.0.2 DMZ-zone
  3  192.168.0.3/24 192.168.0.0 192.168.0.255 Public

[admin@gateway] ip address>
```

- Add a static default route to the local router:
**Configure DMZ server with the ip address of 10.1.0.2, network 10.1.0.1 and gateway address of 10.1.0.1.**

**To make DMZ server accessible from the Internet at address 192.168.0.3 configure dst-nat rule like this:**

```bash
[admin@gateway] ip firewall dst-nat> add action=nat \ 
... dst-address=192.168.0.3/32 to-dst-address=10.1.0.2
```

```bash
[admin@gateway] ip firewall dst-nat> print
Flags: X - disabled, I - invalid, D - dynamic
0 dst-address=192.168.0.3/32 action=nat to-dst-address=10.1.0.2
```