

DefenderMX Appliance Network Setup Instructions

!!! IMPORTANT !!!

Your DefenderMX system must be attached to your network and correctly configured to allow Internet access before attempting to install or configure DefenderMX on the system.

Network Connection:

To begin, please connect your system to the network cable and then:

```
Login as:          root
The password is:   system4me
```

Network Setup:

Then run:

```
redhat-config-network (Red Hat Systems)
```

or

```
system-config-network (CentOS Systems)
```

The screen control keys are:

```
<Tab>/<Alt-Tab> between elements
<Space> selects
<F12> next screen
```

At the first screen select:

```
Run anyway
```

At the second screen select:

```
Ethernet
```

Then select:

```
Configure
```

At the third screen fill-in as shown below:

```
Name          eth0
Device        eth0
Use DHCP      [ ]
Static IP     <enter IP address of your system>
Netmask       255.255.255.0
Default gateway IP <enter IP of your gateway>
```

Then select:

```
OK
```

At the fourth screen select:

```
Exit
```

DNS Setup:

Note: If you are unfamiliar with a Linux text editor please see how to use the nano visual text editor:

<http://www.tqnyc.org/tutorial/nano/index.php?s=>

To set up DNS name resolution, edit the file /etc/resolv.conf

```
nano /etc/resolv.conf
```

Change the contents of the file to read

```
search your-domainname
server ip_address_server1
server ip_address_server2
server ip_address_server3
```

Where:

your-domainname = the DNS name of your domain. i.e. *xsy.com* or *xyz.internal*
ip_address_serverx = The IP address of your DNS server(s)

Please Note:

1. The line:

```
search your-domainname
```

is optional
2. At least one server MUST be specified, two servers are more reliable and up to three server / IP address pairs may be specified.

Hostname configuration:

The set your hostname, edit the file /etc/sysconfig/network

```
nano /etc/sysconfig/network
```

Edit the Line starting with:

```
HOSTNAME=
```

To read:

```
HOSTNAME=your_hostname
```

Please Note:

1. *your_hostname* should be the fully qualified DNS hostname if possible.

Implement Changes:

No need to reboot, just make sure your network cable is connected to eth0 and then run:

```
service network restart
```

No need to reboot, just make sure your network cable is connected to eth0 and then run:

```
Service network restart
```

Firewall considerations:

DCC

The DCC maintainers have been in touch, noting that several sites seem to have set up SpamAssassin and DCC, but have not modified their firewalls to allow DCC traffic through! This is wasting their bandwidth, and we'd appreciate if users could check their configuration.

To check if DCC network connection is working properly, run:

```
cdcc info
```

The output should contain lines like this:

```
dcc1.dcc-servers.net,- RTT+0 ms anon dcc2.dcc-servers.net,
- RTT+0 ms anon ...
```

There should be **at least one**, preferably more than half a dozen, of the public DCC servers listed. If this is not the case, a likely cause is an interfering firewall (see below).

Also note that DCC requires that you open your firewall for DCC reply packets on UDP port 6277. Here's sample firewall rules required:

```
allow udp local gt 1023 to remote 6277
allow udp remote 6277 to local gt 1023
```

DCC IPTables Setup:

IPTables filtering may be enabled directly on a DefenderMX system but it must be configured correctly to allow DCC packets to pass. Assuming you allow all outbound packets out of your machine, you only need to add an INPUT rule to your `/etc/sysconfig/iptables` file. Add the following line in your INPUT chain, above any REJECT rules:

```
-A <chain-name> -p udp -m udp --sport 6277 -j ACCEPT
```

Also, if you're running a large site, processing upwards of hundreds of thousands of messages a day, the DCC maintainers have requested that you consider setting up your own DCC server as described in `dccd(8)`, and arrange to peer with the rest of the public servers.

Razor

The Razor2 system requires outbound access to servers on tcp port 2703 in general (the servers are, at the moment, on the class C 66.151.150.0/24, but allowing only access to those machines would be too restrictive).

It also requires outbound access to those servers on tcp port 7.

It does not require that the razor servers connect to any open ports on your machine. All the connections are typical TCP client connections (ie: from a local port >1023) to port 7 or port 2703 on the razor server.

It does not use UDP or ICMP, with the exception of performing DNS lookups for server discovery.

Pyzor

Pyzor uses both udp and tcp port 24441. It looks as though the client communicates with the server via udp but the server answers back with a tcp connection.

Test System

A simple test will check to see if you will be able to download the required software and updates, After configuring the system as described above, login to the system as root and run:

```
cd /tmp
wget http://www.fsl.com/support/Rules_Du_Jour.tar.gz
```

This should download the file Rules_Du_Jour.tar.gz. You should see something similar to:

```
[root]# wget http://www.fsl.com/support/Rules_Du_Jour.tar.gz
--15:39:37--  http://www.fsl.com/support/Rules_Du_Jour.tar.gz
           => `Rules_Du_Jour.tar.gz'
Resolving www.fsl.com... 69.63.136.146
Connecting to www.fsl.com|69.63.136.146|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 47,377 (46K) [application/x-gzip]

100%[=====>] 47,377
80.47K/s
15:39:39 (80.17 KB/s) - `Rules_Du_Jour.tar.gz' saved
[47377/47377]
```

You may remove the Rules_Du_Jour.tar.gz file after the test.

If you have any problems please contact:

Stephen Swaney
Fort Systems Ltd.
Phone: 202 338-1670
Cell: 202 352-3262
stephen.swaney@fsl.com
www.fsl.com